(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 796 115**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***H04W 12/04*** (2009.01)
***H04W 4/06*** (2009.01)
***H04L 9/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.10.2002 PCT/US2002/32054**

(87) Fecha y número de publicación internacional: **17.04.2003 WO03032573**

(96) Fecha de presentación y número de la solicitud europea: **08.10.2002 E 02776178 (2)**

(97) Fecha y número de publicación de la concesión europea: **08.04.2020 EP 1436939**

(54) Título: **Procedimiento y aparato de seguridad en un sistema de procesamiento de datos**

(30) Prioridad:

**09.10.2001 US 973301**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**25.11.2020**

(73) Titular/es:

**QUALCOMM INCORPORATED (100.0%)**
**5775 Morehouse Drive**
**San Diego, CA 92121, US**

(72) Inventor/es:

**HAWKES, PHILIP;**
**LEUNG, NIKOLAI K., N. y**
**ROSE, GREGORY G.**

(74) Agente/Representante:

**FORTEA LAGUNA, Juan José**

## DESCRIPCIÓN

Procedimiento y aparato de seguridad en un sistema de procesamiento de datos

### ANTECEDENTES

Campo

**[0001]** La presente invención se refiere a sistemas de procesamiento de datos en general y específicamente, a procedimientos y aparatos de seguridad en un sistema de procesamiento de datos.

Antecedentes

**[0002]** La seguridad en el procesamiento de datos y los sistemas de información, incluyendo los sistemas de comunicaciones, contribuye a la responsabilidad, la imparcialidad, la exactitud, la confidencialidad, la operabilidad, así como a una gran cantidad de otros criterios deseados. El cifrado, o el campo general de la criptografía, se usa en comercio electrónico, comunicaciones inalámbricas, radiodifusión y tiene una gama ilimitada de aplicaciones. En el comercio electrónico, el cifrado se usa para evitar fraudes y para verificar transacciones financieras. En los sistemas de procesamiento de datos, el cifrado se usa para verificar la identidad de un participante. El cifrado también se usa para evitar la piratería, proteger páginas web y evitar el acceso a documentos confidenciales, así como una variedad de otras medidas de seguridad.

**[0003]** Los sistemas que emplean criptografía, a menudo denominados criptosistemas, pueden dividirse en criptosistemas simétricos y criptosistemas asimétricos. Un sistema de cifrado simétrico usa una misma clave (es decir, la clave secreta) para cifrar y descifrar un mensaje. No obstante, un sistema de cifrado asimétrico usa una primera clave (es decir, la clave pública) para cifrar un mensaje y usa una segunda clave diferente (es decir, la clave privada) para descifrarlo. Los criptosistemas asimétricos también se denominan criptosistemas de clave pública. Existe un problema en los criptosistemas simétricos en el suministro seguro de la clave secreta de un remitente a un destinatario. Además, existe un problema cuando las claves u otros mecanismos de cifrado se actualizan con frecuencia. En un sistema de procesamiento de datos, los procedimientos de actualización segura de claves generan un tiempo de procesamiento, almacenamiento de memoria y otros costes de procesamiento adicionales. En un sistema de comunicación inalámbrica, la actualización de claves usa un ancho de banda valioso que de otro modo estaría disponible para la transmisión.

**[0004]** La técnica anterior no proporciona un procedimiento para actualizar las claves de un amplio grupo de estaciones móviles para que puedan acceder a una radiodifusión cifrada. Por lo tanto, existe la necesidad de un procedimiento seguro y eficiente para actualizar las claves en un sistema de procesamiento de datos. Además, existe la necesidad de un procedimiento seguro y eficaz para actualizar las claves en un sistema de comunicación inalámbrica.

**[0005]** Se llama la atención además sobre el documento siguiente: Willian Stallings: "Cryptography and Network Security" 1995, Hall Inc., Nueva Jersey, XP 002248261, que proporciona una visión general con respecto a la arquitectura de seguridad de IP, así como a la gestión de claves.

**[0006]** Se llama la atención además al siguiente documento: Menezes, Vanstone, Oorschot, "Handbook of Applied Cryptography", 1997, CRC Press, LLC, EE. UU., páginas 493 a 494, XP 000864288. El documento menciona un protocolo de establecimiento de clave. El protocolo de establecimiento de clave se define como basado en la identidad si la información de identidad de la parte involucrada se usa como clave pública de la parte. El documento también menciona una idea relacionada, en la cual la información de identidad se usa como entrada para la función que determina la clave establecida.

### BREVE EXPLICACIÓN

**[0007]** La invención se define en las reivindicaciones independientes. Algunos modos de realización particulares se exponen en las reivindicaciones dependientes.

### BREVE DESCRIPCIÓN DE LOS DIBUJOS

**[0008]**

La FIG. 1A es un diagrama de un criptosistema.

La FIG. 1B es un diagrama de un criptosistema simétrico.

La FIG. 1C es un diagrama de un criptosistema asimétrico.

La FIG. 1D es un diagrama de un sistema de cifrado de PGP.

La FIG. 1E es un diagrama de un sistema de descifrado de PGP.

La FIG. 2 es un diagrama de un sistema de comunicación de espectro ensanchado que admite un número de usuarios.

La FIG. 3 es un diagrama de bloques del sistema de comunicación que admite transmisiones de radiodifusión.

La FIG. 4 es un diagrama de bloques de una estación móvil en un sistema de comunicación inalámbrica.

Las FIGS. 5A y 5B ilustran modelos que describen la actualización de claves dentro de una estación móvil usada para controlar el acceso de radiodifusión.

La FIG. 6 es un modelo que describe operaciones criptográficas dentro de un UIM.

Las FIGS. 7A-7D ilustran un procedimiento para implementar el cifrado de seguridad en un sistema de comunicación inalámbrica que admite transmisiones de radiodifusión.

La FIG. 7E es un diagrama de temporización de los períodos de actualización de clave de una opción de seguridad en un sistema de comunicación inalámbrica que admite transmisiones de radiodifusión.

Las FIGS. 8A-8D ilustran la aplicación de un procedimiento de cifrado de seguridad en un sistema de comunicación inalámbrica que admite transmisiones de radiodifusión.

La FIG. 9A ilustra el formato de un paquete de IPSec para una transmisión de protocolo de Internet.

La FIG. 9B ilustra un identificador de asociación de seguridad o SPI según corresponda a un paquete de IPSec.

La FIG. 9C ilustra un dispositivo de almacenamiento de memoria para almacenar información del SPI en una estación móvil.

La FIG. 9D ilustra un dispositivo de almacenamiento de memoria para almacenar claves de acceso de radiodifusión (BAK) en una estación móvil.

Las FIGS. 10 y 11 ilustran un procedimiento para proporcionar seguridad para un mensaje de radiodifusión en un sistema de comunicación inalámbrica.

La FIG. 12A ilustra un identificador de asociación de seguridad o SPI según corresponda a un paquete de IPSec.

La FIG. 12B ilustra un dispositivo de almacenamiento de memoria para almacenar información del SPI en una estación móvil.

Las FIGS. 13 y 14 ilustran un procedimiento para proporcionar seguridad para un mensaje de radiodifusión en un sistema de comunicación inalámbrica.

**DESCRIPCIÓN DETALLADA**

**[0009]** El término "ejemplar" se usa de forma exclusiva en el presente documento para significar "que sirve de ejemplo, caso o ilustración". No ha de interpretarse necesariamente que cualquier modo de realización descrito en el presente documento como "ejemplar" sea preferente o ventajoso con respecto a otros modos de realización.

**[0010]** Los sistemas de comunicación inalámbrica están ampliamente desplegados para proporcionar diversos tipos de comunicación, tales como voz, datos, y así sucesivamente. Estos sistemas pueden basarse en el acceso múltiple por división de código (CDMA), el acceso múltiple por división de tiempo (TDMA) o en algunas otras técnicas de modulación. Un sistema de CDMA proporciona determinadas ventajas sobre otros tipos de sistema, incluyendo una mayor capacidad de sistema.

**[0011]** Un sistema puede estar diseñado para admitir uno o más estándares tales como el "estándar de compatibilidad de estaciones base móviles TIA/EIA/IS-95-B para sistema celular de espectro ensanchado y banda ancha en modo dual" denominado en el presente documento como el estándar IS-95, el estándar ofrecido por un consorcio denominado "Proyecto de Colaboración de Tercera Generación" denominado en el presente documento 3GPP, e integrado en un conjunto de documentos que incluyen los documentos números 3G TS 25.211, 3G TS 25.212, 3G TS 25.213 y 3G TS 25.214, el 3G TS 25.302, denominado en el presente documento el estándar W-CDMA, el estándar ofrecido por un consorcio llamado "Segundo Proyecto de Colaboración de Tercera Generación" denominado en el presente documento 3GPP2, y el TR-45.5 denominado en el presente documento el estándar cdma2000,

anteriormente denominado IS-2000 MC. Los estándares citados anteriormente en el presente documento se incorporan en el presente documento expresamente por referencia.

**[0012]** Cada estándar define específicamente el procesamiento de datos para la transmisión desde la estación base al móvil, y viceversa. Como un modo de realización ejemplar, el siguiente análisis considera un sistema de comunicación de espectro ensanchado consecuente con sistemas cdma2000. Los modos de realización alternativos pueden incorporar otro estándar/sistema. Otros modos de realización más pueden aplicar los procedimientos de seguridad divulgados en el presente documento a otro tipo de sistema de procesamiento de datos usando un criptosistema.

**[0013]** Un criptosistema es un procedimiento para disfrazar mensajes que permite que un grupo específico de usuarios extraiga el mensaje. La FIG. 1A ilustra un criptosistema básico 10. La criptografía es la técnica de crear y usar criptosistemas. El criptoanálisis es la técnica de romper criptosistemas, es decir, recibir y comprender el mensaje cuando no se encuentra dentro del grupo específico de usuarios que tienen acceso al mensaje. El mensaje original se conoce como mensaje de texto sin formato o texto sin formato. El mensaje cifrado se denomina texto cifrado, en el que el cifrado incluye cualquier medio para convertir texto sin formato en texto cifrado. El descifrado incluye cualquier medio para convertir el texto cifrado en texto sin formato, es decir, recuperar el mensaje original. Como se ilustra en la FIG. 1A, el mensaje de texto sin formato se cifra para formar un texto cifrado. El texto cifrado se recibe a continuación y se descifra para recuperar el texto sin formato. Si bien los términos texto sin formato y texto cifrado en general se refieren a datos, los conceptos de cifrado pueden aplicarse a cualquier información digital, incluyendo los datos de audio y vídeo presentados en forma digital. Si bien la descripción de la invención proporcionada en el presente documento usa el término texto sin formato y texto cifrado consecuente con la técnica de la criptografía, estos términos no excluyen otras formas de comunicaciones digitales.

**[0014]** Un criptosistema se basa en secretos. Un grupo de entidades comparte un secreto si una entidad fuera de este grupo no puede obtener el secreto sin una gran cantidad de recursos.

**[0015]** Un criptosistema puede ser una colección de algoritmos, en el que cada algoritmo está etiquetado y las etiquetas se llaman claves. Un sistema de cifrado simétrico, a menudo denominado criptosistema, usa una misma clave (es decir, la clave secreta) para cifrar y descifrar un mensaje. Un sistema de cifrado simétrico 20 se ilustra en la FIG. 1B, en el que tanto el cifrado como el descifrado usan una misma clave privada.

**[0016]** Por el contrario, un sistema de cifrado asimétrico usa una primera clave (por ejemplo, la clave pública) para cifrar un mensaje y usa una clave diferente (por ejemplo, la clave privada) para descifrarlo. La FIG. 1C ilustra un sistema de cifrado asimétrico 30 en el que se proporciona una clave para el cifrado y una segunda clave para el descifrado. Los criptosistemas asimétricos también se denominan criptosistemas de clave pública. La clave pública se publica y está disponible para cifrar cualquier mensaje, sin embargo, solo la clave privada se puede usar para descifrar el mensaje cifrado con la clave pública.

**[0017]** Existe un problema en los criptosistemas simétricos en el suministro seguro de la clave secreta de un remitente a un destinatario. En una solución, se puede usar un servicio de mensajería para proporcionar la información, o una solución más eficaz y confiable puede ser usar un criptosistema de clave pública, tal como un criptosistema de clave pública definido por Rivest, Shamir y Adleman (RSA) que se analiza a continuación en el presente documento. El sistema RSA se usa en la popular herramienta de seguridad denominada Pretty Good Privacy [Privacidad Bastante Buena] (PGP, por sus siglas en inglés), que se detalla más a continuación en el presente documento. Por ejemplo, un criptosistema originalmente registrado alteró letras en un texto sin formato al cambiar cada letra por *n* en el alfabeto, en el que *n* es un valor entero constante predeterminado. En dicho esquema, una "A" se reemplaza por una "D", etc., en el que un esquema de cifrado dado puede incorporar varios valores diferentes de *n.* En este esquema de cifrado, "*n*" es la clave. Los destinatarios previstos reciben el esquema de cifrado antes de recibir un texto cifrado. De esta manera, solo aquellos que conozcan la clave deberían poder descifrar el texto cifrado para recuperar el texto sin formato. Sin embargo, al calcular la clave con conocimiento de cifrado, las partes no deseadas pueden interceptar y descifrar el texto cifrado, creando un problema de seguridad.

**[0018]** Los criptosistemas más complicados y sofisticados emplean claves estratégicas que impiden la intercepción y descifrado por parte de partes no deseadas. Un criptosistema clásico emplea funciones de cifrado *E* y funciones de descifrado *D* de modo que:

$$D\_K(E\_K(P)) = P, \text{ para cualquier texto sin formato } P. \qquad (1)$$

**[0019]** En un criptosistema de clave pública, E_K se calcula fácilmente a partir de una "clave pública" conocida *Y,* que a su vez se calcula a partir de *K.* La clave pública *Y* se publica, de modo que cualquiera pueda cifrar mensajes. La función de descifrado D_K se calcula a partir de la clave pública *Y,* pero solo con el conocimiento de una clave privada *K.* Sin la clave privada *K,* un destinatario no deseado no puede descifrar el texto cifrado generado de este modo. De esta forma, solo el destinatario que generó *K* puede descifrar mensajes.

**[0020]** RSA es un criptosistema de clave pública definido por Rivest, Shamir y Adleman, en el que, por ejemplo, los textos sin formato consideran números enteros positivos hasta $2^{512}$. Las claves son cuádruples (*p, q, e, d*), con *p* dado como número primo de 256 bits, *q* como número primo de 258 bits, y *d* y e números grandes con (*de* - 1) divisible por (*p*-1)(*q*-1). Además, definen la función de cifrado como:

$$E\_K(P) = P^e \bmod pq,\ D\_K(C) = C^d \bmod pq. \qquad (2)$$

**[0021]** Si bien E_K se calcula fácilmente a partir del par (*pq,e*), no se conoce una forma simple de calcular D_K a partir del par (*pq,e*). Por lo tanto, el destinatario que genera K puede publicar (*pq,e*). Es posible enviar un mensaje secreto al destinatario ya que él es el que puede leer el mensaje.

**[0022]** La PGP combina características de cifrado simétrico y asimétrico. Las FIGS. 1D y 1E ilustran un criptosistema de PGP 50, en el que un mensaje de texto sin formato se cifra y se recupera. En la FIG. 1D, el mensaje de texto sin formato se comprime para ahorrar tiempo de transmisión del módem y espacio en el disco. La compresión fortalece la seguridad criptográfica al agregar otro nivel de traducción al procesamiento de cifrado y descifrado. La mayoría de las técnicas de criptoanálisis explotan patrones encontrados en el texto sin formato para descifrar el cifrado. La compresión reduce estos patrones en el texto sin formato, mejorando de este modo la resistencia al criptoanálisis. Debe observarse que un modo de realización no comprime: texto sin formato u otros mensajes que son demasiado cortos para comprimir o que no se comprimen bien.

**[0023]** La PGP crea a continuación una clave de sesión, que es una clave secreta de un solo uso. Esta clave es un número aleatorio que puede generarse a partir de cualquier evento aleatorio, tal como los movimientos aleatorios de un ratón de ordenador y/o las pulsaciones de teclas mientras se escribe. La clave de sesión funciona con un algoritmo de cifrado seguro para cifrar el texto sin formato, lo que da como resultado un texto cifrado. Una vez que los datos se cifran, la clave de sesión se cifra a continuación a la clave pública del destinatario. La clave de sesión cifrada con clave pública se transmite junto con el texto cifrado al destinatario.

**[0024]** Para descifrar, como se ilustra en la FIG. 1E, la copia de PGP del destinatario usa una clave privada para recuperar la clave de sesión temporal, que la PGP usa a continuación para descifrar el texto cifrado convencionalmente encriptado. La combinación de procedimientos de cifrado aprovecha la conveniencia del cifrado de clave pública y la velocidad del cifrado simétrico. El cifrado simétrico es en general mucho más rápido que el cifrado de clave pública. El cifrado de clave pública a su vez proporciona una solución a los problemas de distribución de claves y transmisión de datos. En combinación, el rendimiento y la distribución de claves se mejoran sin sacrificar la seguridad.

**[0025]** Una clave es un valor que funciona con un algoritmo criptográfico para producir un texto cifrado específico. Las claves son básicamente números muy grandes. El tamaño de la clave se mide en bits. En la criptografía de clave pública, la seguridad aumenta con el tamaño de la clave, sin embargo, el tamaño de la clave pública y el tamaño de la clave privada de cifrado simétrico en general no están relacionados. Si bien las claves públicas y privadas están relacionadas matemáticamente, surge una dificultad para derivar una clave privada dada a partir de solo una clave pública. Es posible obtener la clave privada con el tiempo suficiente y la potencia de cálculo, lo que hace que la selección del tamaño de la clave sea un problema de seguridad importante. El objetivo óptimo es maximizar el tamaño de la clave por cuestiones de seguridad, mientras se minimiza el tamaño de la clave para facilitar el procesamiento rápido. Las claves más grandes serán criptográficamente seguras durante un período de tiempo más largo. Una consideración adicional es el interceptor esperado, específicamente: 1) cuál es la importancia de un mensaje a un tercero; y 2) cuánto recurso tendrá un tercero para descifrar el mensaje.

**[0026]** Debe observarse que las claves se almacenan en forma cifrada. La PGP almacena específicamente claves en dos archivos: uno para claves públicas y otro para claves privadas. Estos archivos se llaman llaveros. En la aplicación, un sistema de cifrado PGP agrega las claves públicas de los destinatarios diana al llavero público del remitente. Las claves privadas del remitente se almacenan en el llavero privado del remitente.

**[0027]** Como se analiza en los ejemplos dados anteriormente en el presente documento, el procedimiento de distribución de las claves usadas para el cifrado y descifrado puede ser complicado. El "problema de intercambio de claves" implica primero garantizar que las claves se intercambien de modo que tanto el emisor como el receptor puedan realizar el cifrado y descifrado, respectivamente, y para la comunicación bidireccional, de modo que el emisor y el receptor puedan cifrar y descifrar mensajes. Además, se desea que el intercambio de claves se realice para evitar la intercepción de una tercera parte no prevista.

**[0028]** Finalmente, una consideración adicional es la autenticación, que garantiza al receptor que un mensaje fue cifrado por un remitente previsto y no por un tercero. En un sistema de intercambio de claves privadas, las claves se intercambian en secreto proporcionando una seguridad mejorada tras un intercambio de claves exitoso y una autenticación válida. Debe observarse que el esquema de cifrado de clave privada proporciona implícitamente autenticación. La suposición subyacente en un criptosistema de clave privada es que solo el remitente previsto tendrá la clave capaz de cifrar los mensajes entregados al receptor previsto. Si bien los procedimientos criptográficos de clave pública resuelven un aspecto crítico del "problema del intercambio de claves', específicamente su resistencia al análisis

incluso con la presencia de un espía pasivo durante el intercambio de claves, siguen sin resolver todos los problemas asociados con el intercambio de claves. En particular, dado que las claves se consideran de 'conocimiento público' (particularmente con RSA), se desea algún otro mecanismo para proporcionar autenticación. La autenticación se desea como posesión de claves por sí sola, aunque es suficiente para cifrar mensajes, no es una prueba de una identidad única particular del remitente, ni la posesión de una clave de descifrado correspondiente por sí misma es suficiente para establecer la identidad del destinatario.

**[0029]** Una solución es desarrollar un mecanismo de distribución de claves que garantice que las claves enumeradas sean en realidad las de las entidades dadas, a veces denominadas autoridad de confianza, autoridad de certificación o agente de custodia de terceros. Realmente, la autoridad típicamente no genera claves, pero se asegura de que las listas de claves y las identidades asociadas que los remitentes y receptores mantienen y anuncian como referencia sean correctas y no estén comprometidas. Otro procedimiento se basa en que los usuarios distribuyan y rastreen las claves de los demás y confíen de manera informal y distribuida. Bajo RSA, si un usuario desea enviar una prueba de su identidad además de un mensaje cifrado, se cifra una firma con la clave privada. El receptor puede usar el algoritmo de RSA a la inversa para verificar que la información se descifra, de modo que solo el remitente podría haber cifrado el texto sin formato mediante el uso de la clave secreta. Típicamente, la "firma" cifrada es un "compendio de mensaje" que comprende un 'resumen' matemático único del mensaje secreto (si la firma fuera estática en varios mensajes, una vez conocida, receptores anteriores podrían usarla falsamente). De esta manera, teóricamente, solo el remitente del mensaje podría generar una firma válida para ese mensaje, autenticándolo de este modo para el receptor.

**[0030]** Un compendio de mensaje a menudo se calcula usando una función hash criptográfica. Una función hash criptográfica calcula un valor (con un número fijo de bits) de cualquier entrada, independientemente de la longitud de la entrada. Una propiedad de una función hash criptográfica es esta: dado un valor de salida, es computacionalmente difícil determinar una entrada que dará como resultado esa salida. Un ejemplo de una función hash criptográfica es SHA-1 como se describe en "Secure Hash Standard" [Estándar de Hash Seguro], FIPS PUB 180-1, promulgado por las Publicaciones de estándares de procesamiento de información federal (FIPS PUBS) y emitido por el Instituto Nacional de Estándares y Tecnología.

**[0031]** La FIG. 2 sirve como ejemplo de un sistema de comunicaciones 100 que admite un número de usuarios y puede implementar al menos algunos aspectos y modos de realización de la invención. Se puede usar cualquiera de una variedad de algoritmos y procedimientos para planificar transmisiones en el sistema 100. El sistema 100 proporciona la comunicación para un número de celdas 102A a 102G, cada una de las cuales recibe el servicio por una estación base correspondiente 104A a 104G, respectivamente. En el modo de realización ejemplar, algunas estaciones base 104 tienen múltiples antenas receptoras y otras tienen solamente una antena receptora. De forma análoga, algunas de las estaciones base 104 tienen múltiples antenas transmisoras, y otras tienen antenas transmisoras individuales. No existen restricciones sobre las combinaciones de las antenas transmisoras y las antenas receptoras. Por lo tanto, es posible que una estación base 104 tenga múltiples antenas de transmisión y una sola antena de recepción, o que tenga múltiples antenas de recepción y una sola antena de transmisión, o que tenga antenas de transmisión y de recepción tanto individuales como múltiples.

**[0032]** Los terminales 106A, 106B, 106C, 106D, 106E, 106F, 106G, 106H y 106I en el área de cobertura pueden ser fijos (es decir, estacionarios) o móviles. Como se muestra en la FIG. 2, diversos terminales 106 se encuentran dispersos por todo el sistema. Cada terminal 106 se comunica con al menos una y posiblemente más estaciones base 104 por el enlace descendente y el enlace ascendente en cualquier momento determinado dependiendo, por ejemplo, de si se emplea un traspaso suave o si el terminal se encuentra diseñado y operado para recibir (simultánea o secuencialmente) múltiples transmisiones procedentes de múltiples estaciones base. El traspaso suave en sistemas de comunicaciones de CDMA es bien conocido en la técnica y se describe en detalle en la patente de los EE. UU. N.º 5.101.501, titulada "Method and system for providing a Soft Handoff In a CDMA Cellular Telephone System [Procedimiento y sistema para proporcionar un traspaso suave en un sistema de teléfono celular de CDMA]", que está cedida al cesionario de la presente invención.

**[0033]** El enlace descendente se refiere a la transmisión desde la estación base al terminal, y el enlace ascendente se refiere a la transmisión desde el terminal a la estación base. En el modo de realización ejemplar, algunos de los terminales 106 tienen múltiples antenas receptoras y otros tienen solamente una antena receptora. En la FIG. 2, la estación base 104A transmite los datos a los terminales 106A y 106J en el enlace descendente, la estación base 104B transmite datos a los terminales 106B y 106J, la estación base 104C transmite datos al terminal 106C, y así sucesivamente.

**[0034]** La creciente demanda de transmisión de datos inalámbrica y la expansión de servicios disponibles a través de la tecnología de comunicación inalámbrica han conducido al desarrollo de servicios de datos específicos. Uno de estos servicios se conoce como alta velocidad de datos (HDR). Se propone un servicio de HDR ejemplar en "EIA/TIA-IS856 cdma2000 High Rate Packet Data Air Interface Specification", denominado "la memoria descriptiva de HDR". El servicio de HDR es en general una superposición a un sistema de comunicación de voz que proporciona un procedimiento eficaz para transmitir paquetes de datos en un sistema de comunicación inalámbrica. A medida que aumenta la cantidad de datos transmitidos y la cantidad de transmisiones, el ancho de banda limitado disponible para las transmisiones de radio se convierte en un recurso crítico. Por lo tanto, existe la necesidad de un procedimiento

eficaz y justo para planificar transmisiones en un sistema de comunicación que optimice el uso del ancho de banda disponible. En el modo de realización ejemplar, el sistema 100 que se ilustra en la FIG. 2 es consecuente con un sistema de tipo CDMA que tiene servicio de HDR.

**[0035]** De acuerdo con un modo de realización, el sistema 100 admite un servicio de radiodifusión multimedia a alta velocidad denominado servicio de radiodifusión a alta velocidad (HSBS). Una aplicación ejemplar para HSBS es la transmisión en continuo de vídeo de películas, eventos deportivos, etc. El servicio de HSBS es un servicio de datos en paquetes basado en el protocolo de Internet (IP). De acuerdo con el modo de realización ejemplar, un proveedor de servicios indica la disponibilidad de dicho servicio de radiodifusión a alta velocidad para los usuarios. Los usuarios que desean el servicio HSBS se abonan para recibir el servicio y pueden descubrir la programación del servicio de radiodifusión a través de anuncios, sistema de gestión breve (SMS), protocolo de aplicación inalámbrica (WAP), etc. Los usuarios móviles se denominan estaciones móviles (MS). Las estaciones base (BS) transmiten parámetros relacionados con el HSBS en mensajes de sobrecarga. Cuando una MS desea recibir la sesión de radiodifusión, la MS lee los mensajes de sobrecarga y aprende las configuraciones apropiadas. La MS sintoniza la frecuencia que contiene el canal de HSBS y recibe el contenido del servicio de radiodifusión.

**[0036]** El servicio que se está considerando es un servicio de radiodifusión multimedia de alta velocidad. Este servicio se conoce como servicio de radiodifusión a alta velocidad (HSBS) en este documento. Un ejemplo de ello es la transmisión en continuo de vídeo de películas, eventos deportivos, etc. Es probable que este servicio sea un servicio de datos en paquetes basado en el protocolo de Internet (IP).

**[0037]** El proveedor de servicios indicará la disponibilidad de dicho servicio de radiodifusión a alta velocidad a los usuarios. Los usuarios de estaciones móviles que deseen dicho servicio se abonarán para recibir este servicio y pueden descubrir la programación del servicio de radiodifusión a través de anuncios, SMS; WAP, etc. Las estaciones base transmitirán parámetros relacionados con el servicio de radiodifusión en mensajes de sobrecarga. Los móviles que deseen escuchar la sesión de radiodifusión leerán estos mensajes para determinar las configuraciones apropiadas, sintonizarán la frecuencia que contiene el canal de radiodifusión a alta velocidad y comenzarán a recibir el contenido del servicio de radiodifusión.

**[0038]** Existen varios modelos posibles de abono/ingresos para el servicio de HSBS, que incluyen acceso gratuito, acceso controlado y acceso parcialmente controlado. Para el acceso gratuito, no se necesita abono para que los móviles reciban el servicio. La BS difunde el contenido sin cifrado y los móviles interesados pueden recibir el contenido. Los ingresos para el proveedor de servicios pueden generarse a través de anuncios que también pueden transmitirse en el canal de radiodifusión. Por ejemplo, se pueden transmitir los próximos tráilers de película por los cuales los estudios pagarán al proveedor de servicios.

**[0039]** Para el acceso controlado, los usuarios de MS se abonan al servicio y pagan la tarifa correspondiente para recibir el servicio de radiodifusión. Los usuarios que no están abonados al servicio no pueden recibir el servicio de HSBS. El acceso controlado se puede lograr cifrando la transmisión/contenido de HSBS de modo que solo los usuarios abonados puedan descifrar el contenido. Este puede usar procedimientos de intercambio de claves de cifrado por aire. Este esquema proporciona una seguridad robusta e impide el robo de servicio.

**[0040]** Un esquema de acceso híbrido, denominado acceso controlado parcial, proporciona el servicio de HSBS como un servicio basado en abono que se cifra con transmisiones publicitarias intermitentes sin cifrar. Estos anuncios pueden estar destinados a fomentar los abonos al servicio de HSBS cifrado. La programación de dichos segmentos sin cifrar podría ser conocida por la MS a través de medios externos.

**[0041]** Un sistema de comunicación inalámbrica 200 se ilustra en la FIG. 3, en el que se proporciona información de vídeo y audio a la red de servicio de datos empaquetados (PDSN) 202 por parte de un servidor de contenido (CS) 201. La información de vídeo y audio puede ser de programación televisada o una transmisión de radio. La información se proporciona como datos empaquetados, tales como en paquetes IP. La PDSN 202 procesa los paquetes IP para su distribución dentro de una red de acceso (AN). Como se ilustra, la AN se define como las partes del sistema que incluyen una BS 204 en comunicación con múltiples MS 206. La PDSN 202 está acoplada a la BS 204. Para el servicio de HSBS, la BS 204 recibe el flujo de información de la PDSN 202 y proporciona la información en un canal designado a los abonados dentro del sistema 200. Para controlar el acceso, el contenido es cifrado por el CS 201 antes de ser proporcionado a la PDSN 202. Los usuarios abonados son provistos de la clave de descifrado de modo que los paquetes IP puedan descifrarse.

**[0042]** La FIG. 4 detalla una MS 300, similar a la MS 206 de la FIG. 3. La MS 300 tiene una antena 302 acoplada a los circuitos de recepción 304. La MS 300 recibe transmisiones de una BS (no mostrada) similar a la BS 204 de la FIG. 3. La MS 300 incluye un módulo de identificación de usuario (UIM) 308 y un equipo móvil (ME) 306. Los circuitos de recepción están acoplados al UIM 308 y al ME 306. El UIM 308 aplica procedimientos de verificación para la seguridad de la transmisión de HSBS y proporciona diversas claves para el ME 306. El ME 306 puede estar acoplado a la unidad de procesamiento 312. El ME 306 realiza un procesamiento sustancial, que incluye, pero no se limita a, descifrado de secuencias de contenido de HSBS. El ME 306 incluye una unidad de almacenamiento de memoria, MEM 310. En el modo de realización ejemplar, un no abonado puede acceder fácilmente a los datos en la unidad de

procesamiento del ME 306 (no mostrada) y los datos en la unidad de almacenamiento de memoria del ME, MEM 310 mediante el uso de recursos limitados y, por lo tanto, se dice que el ME 306 es inseguro. Cualquier información transmitida al ME 306 o procesada por el ME 306 permanece en secreto de forma segura por un corto período de tiempo. Por lo tanto, se desea que cualquier información secreta, tal como una clave o claves, compartida(s) con el ME 306 se cambie con frecuencia.

**[0043]** Se confía en el UIM 308 para almacenar y procesar información secreta (tal como claves de cifrado) que debe permanecer en secreto durante mucho tiempo. Como el UIM 308 es una unidad segura, los secretos almacenados en el mismo no necesariamente requieren que el sistema cambie la información secreta con frecuencia. El UIM 308 incluye una unidad de procesamiento denominada unidad de procesamiento de UIM segura (SUPU) 316 y una unidad de almacenamiento de memoria denominada unidad de memoria de UIM segura (SUMU) 314 que se considera segura. Dentro del UIM 308, la SUMU 314 almacena información secreta de tal manera que se desaliente el acceso no autorizado a la información. Si la información secreta se obtiene del UIM 308, el acceso requerirá una cantidad significativamente grande de recursos. También dentro del UIM 308, la SUPU 316 realiza cálculos sobre valores que pueden ser externos al UIM 308 y/o internos al UIM 308. Los resultados del cálculo pueden almacenarse en la SUMU 314 o transferirse al ME 306. Los cálculos realizados con la SUPU 316 solo pueden obtenerse del UIM 308 por una entidad con una cantidad significativamente grande de recursos. De forma similar, las salidas de la SUPU 316 que están designadas para ser almacenadas dentro de la SUMU 314 (pero no las salidas al ME 306) están diseñadas de modo que la intercepción no autorizada requiere una cantidad significativamente grande de recursos. En un modo de realización, el UIM 308 es una unidad estacionaria dentro de la MS 300. Debe observarse que, además de la memoria segura y el procesamiento dentro del UIM 308, el UIM 308 también puede incluir memoria y procesamiento no seguros (no mostrados) para almacenar información, incluyendo números de teléfono, información de dirección de correo electrónico, página web o información de dirección URL, y/o funciones de programación, etc.

**[0044]** Modos de realización alternativos pueden proporcionar un UIM extraíble y/o reprogramable. En el modo de realización ejemplar, la SUPU 316 no tiene una potencia de procesamiento significativa para funciones más allá de los procedimientos de seguridad y clave, en el que los procedimientos de seguridad y clave se pueden usar típicamente para permitir el cifrado del contenido de radiodifusión del HSBS. Modos de realización alternativos pueden implementar un UIM que tenga una potencia de procesamiento más fuerte.

**[0045]** El UIM 308 está asociado con un usuario particular y se usa principalmente para verificar que la MS 300 tiene derecho a los privilegios otorgados al usuario, tal como el acceso a la red de telefonía móvil. Por lo tanto, un usuario está asociado con el UIM 308 en lugar de una MS 300. El mismo usuario puede estar asociado con múltiples UIM 308.

**[0046]** El servicio de radiodifusión enfrenta un problema para determinar cómo distribuir las claves a los usuarios abonados. Para descifrar el contenido de radiodifusión en un momento determinado, el ME tiene que conocer la clave de descifrado actual. Para evitar el robo del servicio, la clave de descifrado se debe cambiar con frecuencia, por ejemplo, un servicio actualiza la clave cada minuto. Estas claves de descifrado se denominan claves a corto plazo (SK). La SK se usa para descifrar el contenido de radiodifusión durante un corto período de tiempo, por lo que se puede suponer que la SK tiene cierto valor monetario intrínseco para un usuario. Por ejemplo, este valor monetario intrínseco puede ser una parte de los costes de registro. Se supone que el coste de un no abonado que obtiene la SK de la unidad de almacenamiento de memoria de MEM 310 de un abonado excede el valor monetario intrínseco de la SK. Es decir, el coste de obtener ilegítimamente la SK excede la recompensa, lo que no da como resultado ningún beneficio neto. En consecuencia, se reduce la necesidad de proteger la SK en la unidad de almacenamiento de memoria de MEM 310. Sin embargo, si una clave secreta tiene una vida útil más larga que la de la SK, el coste de obtener esta clave secreta ilegítimamente puede ser menor que la recompensa. En esta situación, existe un beneficio neto al obtener de forma ilegítima dicha clave de la unidad de almacenamiento de memoria de MEM 310. Por lo tanto, idealmente, la unidad de almacenamiento de memoria de MEM 310 no almacenará secretos con una vida útil más larga que la de la SK.

**[0047]** Se supone que los canales usados por el CS (no mostrados) para distribuir la SK a las diversas unidades de abonado son inseguros. En otras palabras, un diseño óptimo supondrá que los canales son inseguros y diseñará la SK en consecuencia. Por lo tanto, al distribuir una SK dada, el CS desea usar una técnica que oculte el valor de la SK a los usuarios no abonados. Además, el CS distribuye la SK a cada uno de un número potencialmente grande de abonados para su procesamiento en los ME respectivos dentro de un intervalo relativamente corto. Los procedimientos seguros conocidos de transmisión de claves son tradicionalmente lentos y requieren la transmisión de una gran cantidad de claves. Los procedimientos de transmisión de clave en general no son factibles para la combinación deseada de criterios de seguridad y eficacia. El modo de realización ejemplar es un procedimiento factible de distribuir claves de descifrado a un gran conjunto de abonados dentro de un intervalo pequeño de tal manera que los no abonados no puedan obtener las claves de descifrado.

**[0048]** El modo de realización ejemplar se describe como la transmisión de información en paquetes compatibles con el protocolo de Internet, tales como paquetes "IPSec" como se describe a continuación en el presente documento, y por lo tanto, la siguiente descripción proporciona una breve introducción a la terminología usada en asociación con el IPSec. Esta terminología es útil para describir modos de realización ejemplares, pero el uso de esta terminología no pretende limitar el modo de realización ejemplar a las comunicaciones que usan IPSec.

**[0049]** Los fundamentos de IPSec se especifican en RFC 1825 titulado "Security Architecture for the Internet Protocol" por R. Atkinson en agosto de 1995, RFC 1826 titulado "IP Authentication Header" por R. Atkinson en agosto de 1995, y RFC 1827 titulado "IP Encapsulating Security Payload (ESP)" por R. Atkinson en agosto de 1995. La cabecera de autenticación es un mecanismo para proporcionar integridad a los datagramas de IP, en el que los datagramas de IP en general son una recopilación de información útil, denominada carga útil, combinada con información de control de red y una cabecera de IP. Los enrutadores de red usan la cabecera de IP para dirigir el paquete al nodo de red apropiado. En algunas circunstancias, la cabecera de autenticación también puede proporcionar autenticación a datagramas de IP. La ESP es un mecanismo para proporcionar confidencialidad e integridad a los datagramas de IP, y se puede usar junto con la cabecera de autenticación. El IPSec usa "asociaciones de seguridad" para describir los parámetros, tal como la clave de cifrado y el algoritmo de cifrado, usados para cifrar y/o autenticar comunicaciones entre un grupo de entidades. Debe observarse que el concepto de una asociación de seguridad también es válido cuando se aplica a criptosistemas que no están basados en IPSec.

**[0050]** Un paquete de IPSec incluye un parámetro de 32 bits llamado Índice de Parámetros de Seguridad (SPI) que se usa, junto con la dirección de destino, para identificar la asociación de seguridad usada para cifrar y/o autenticar el contenido del datagrama de IP. Una entidad puede almacenar las asociaciones de seguridad en una base de datos de asociaciones de seguridad e indexar las asociaciones de seguridad de acuerdo con la dirección de destino y el SPI. El contenido cifrado de un paquete de IPSec a menudo se denomina carga útil.

**[0051]** En el modo de realización ejemplar, la MS 300 soporta el HSBS en un sistema de comunicación inalámbrica. Para obtener acceso al HSBS, el usuario debe registrarse y a continuación abonarse al servicio. Una vez que se habilita el abono, las diversas claves se actualizan según sea necesario. En el proceso de registro, el CS y el UIM 308 negocian una asociación de seguridad y acuerdan una clave de registro (RK) y otros parámetros necesarios para la asociación de seguridad entre el usuario y el CS. El CS puede enviar a continuación al UIM 308 más información secreta cifrada con la RK. La RK se mantiene como secreto en el UIM 308, mientras que otros parámetros se pueden guardar en el ME 306. La RK es exclusiva de un UIM 308 dado, es decir, a cada usuario se le asigna una RK diferente. El proceso de registro por sí solo no le da acceso al usuario al HSBS.

**[0052]** Como se indica anteriormente en el presente documento, después de registrarse, el usuario se abona al servicio. En el proceso de abono, el CS envía al UIM 308 el valor de una clave de acceso de radiodifusión común (BAK). Debe observarse que mientras que la RK es específica para el UIM 308, la BAK se usa para cifrar un mensaje de radiodifusión a múltiples usuarios. El CS envía a la MS 300, y específicamente al UIM 308, el valor de la BAK, cifrado usando la RK exclusiva del UIM 308. El UIM 308 puede recuperar el valor de la BAK original de la versión cifrada usando la RK. La BAK, junto con otros parámetros, forman una asociación de seguridad entre el CS y el grupo de usuarios abonados. La BAK se mantiene como secreto en el UIM 308, mientras que otros parámetros de la asociación de seguridad pueden mantenerse en el ME 306. El CS radiodifunde a continuación datos llamados Información de SK (SKI) que se combinan con la BAK en el UIM 308 para derivar la SK. A continuación, el UIM 308 transmite la SK al ME 306. De esta manera, el CS puede distribuir eficazmente nuevos valores de SK al ME de los usuarios abonados. A continuación, en el presente documento se presentan varios ejemplos de cómo la SK se deriva de la SKI y las formas que puede tomar la SKI. Los procesos de registro y abono se analizan en detalle, después de lo cual se describen la SKI y la SK.

**[0053]** Con respecto al registro, cuando un usuario se registra con un CS determinado, el UIM 308 y el CS (no mostrado) establecen una asociación de seguridad. Es decir, el UIM 308 y el CS acuerdan una clave de registro secreta RK. La RK es única para cada UIM 308, aunque si un usuario tiene múltiples UIM, estos UIM pueden compartir la misma RK dependiendo de las políticas del CS. Este registro se puede producir cuando el usuario se abona a un canal de radiodifusión ofrecido por el CS o se puede producir antes del abono. Un solo CS puede ofrecer múltiples canales de radiodifusión. El CS puede optar por asociar al usuario con la misma RK para todos los canales o requerir que el usuario se registre para cada canal y asocie al mismo usuario con diferentes RK en diferentes canales. Múltiples CS pueden elegir usar las mismas claves de registro o requerir que el usuario se registre y obtenga una RK diferente para cada CS.

**[0054]** Los tres escenarios comunes para configurar esta asociación de seguridad incluyen: 1) el procedimiento de acuerdo de clave autenticada (AKA) que se usa en sistemas 3GPP; 2) el procedimiento de intercambio de claves de Internet (IKE) como se usa en IPSec; y 3) aprovisionamiento de servicios por aire (OTASP). En cualquier caso, la unidad de memoria de UIM SUMU 314 contiene una clave secreta denominada en el presente documento la clave A. Por ejemplo, usando el procedimiento de AKA, la clave A es un secreto conocido solo por el UIM y un tercero de confianza (TTP), en el que el TTP puede consistir en más de una entidad. El TTP es típicamente el proveedor de servicios móviles con el que está registrado el usuario. Toda la comunicación entre el CS y el TTP es segura, y el CS confía en que el TTP no ayudará con el acceso no autorizado al servicio de radiodifusión. Cuando el usuario se registra, el CS informa al TTP que el usuario desea registrarse para el servicio y proporciona una verificación de la solicitud del usuario. El TTP usa una función, similar a una función hash criptográfica, para calcular la RK a partir de la tecla A y datos adicionales llamados Información de clave de registro (RKI). El TTP pasa la RK y/o RKI al CS a través de un canal seguro junto con otros datos. El CS envía la RKI a la MS 300. Los circuitos de recepción 304 transmiten la RKI al UIM 308 y pueden transmitir la RKI al ME 306. El UIM 308 calcula la RK a partir de la RKI y la tecla A que se

almacena en la unidad de memoria de UIM SUMU 314. La RK se almacena en la unidad de memoria de UIM SUMU 314 y no se proporciona directamente al ME 306. Los modos de realización alternativos pueden usar un escenario de IKE o algún otro procedimiento para establecer la RK. Los otros parámetros de la asociación de seguridad entre el CS y el UIM 308 también deben negociarse. La RK se mantiene como secreto en el UIM 308, mientras que otros parámetros de la asociación de seguridad pueden mantenerse en el ME 306. En el modo de realización ejemplar, en el que la BAK se envía al UIM 308 como un paquete IPSec cifrado usando RK, el CS y la MS 300 negocian un valor de SPI usado para indexar la asociación de seguridad y este SPI se denomina SPI_RK.

**[0055]** En el procedimiento de AKA, la RK es un secreto compartido entre el CS, el UIM y el TTP. Por lo tanto, como se usa en el presente documento, el procedimiento de AKA implica que cualquier asociación de seguridad entre CS y UIM incluye implícitamente el TTP. La inclusión del TTP en cualquier asociación de seguridad no se considera una violación de la seguridad, ya que el CS confía en que el TTP no ayudará en el acceso no autorizado al canal de radiodifusión. Como se indica anteriormente en el presente documento, si se comparte una clave con el ME 306, es conveniente cambiar esa clave con frecuencia. Esto se debe al riesgo de que un no abonado acceda a la información almacenada en la unidad de almacenamiento de memoria de MEM 310 y, por tanto, permita el acceso a un servicio controlado o parcialmente controlado. El ME 306 almacena la SK, es decir, la información de clave usada para descifrar contenido de radiodifusión, en la unidad de almacenamiento de memoria de MEM 310. El CS envía información suficiente para que los usuarios abonados calculen la SK. Si el ME 306 de un usuario abonado puede calcular la SK a partir de esta información, entonces la información adicional requerida para calcular la SK no puede ser secreta. En este caso, se supone que el ME 306 de un usuario no abonado también podría calcular la SK a partir de esta información. Por lo tanto, el valor de SK debe calcularse en la SUPU 316, usando una clave secreta compartida por el CS y la SUMU 314. El CS y la SUMU 314 comparten el valor de RK, sin embargo, cada usuario tiene un valor único de RK. El CS no tiene tiempo suficiente para cifrar la SK con cada valor de RK y transmitir estos valores cifrados a cada usuario abonado.

**[0056]** Con respecto al abono, para garantizar la distribución eficaz de la información de seguridad de SK, el CS distribuye periódicamente una clave de acceso de radiodifusión (BAK) común a cada UIM de abonado 308. Para cada abonado, el CS cifra la BAK usando la RK correspondiente para obtener un valor llamado Información BAKI (BAKI). El CS envía la BAKI correspondiente a la MS 300 del usuario abonado. Por ejemplo, la BAK puede transmitirse como un paquete de IP cifrado usando la RK correspondiente a cada MS. En el modo de realización ejemplar, la BAKI es un paquete de IPSec que contiene la BAK que se cifra usando la RK como clave. Como la RK es una clave por usuario, el CS debe enviar la BAK a cada abonado individualmente; por tanto, la BAK no se envía a través del canal de radiodifusión. La MS 300 transmite la BAKI al UIM 308. La SUPU 316 calcula la BAK usando el valor de RK almacenado en la SUMU 314 y el valor de BAKI. El valor de BAK se almacena a continuación en la SUMU. En el modo de realización ejemplar, la BAKI contiene un valor de SPI denotado SPI_RK que corresponde a la asociación de seguridad que contiene RK. La MS 300 sabe que el UIM 308 puede descifrar la carga útil cuando el paquete de IPSec se cifra de acuerdo con esta asociación de seguridad. En consecuencia, cuando la MS 300 recibe un paquete de IPSec cifrado de acuerdo con esta asociación de seguridad, la MS 300 pasa la BAKI al UIM 308, e indica al UIM 308 que use la RK para descifrar la carga útil.

**[0057]** Se desea que el período para actualizar la BAK sea suficiente para permitir que el CS envíe la BAK a cada abonado individualmente, sin incurrir en una sobrecarga significativa. Dado que no se confía en el ME 306 para guardar secretos durante mucho tiempo, el UIM 308 no proporciona la BAK al ME 306. Los otros parámetros de la asociación de seguridad entre el CS y el grupo de abonados también deben negociarse. En un modo de realización, estos parámetros son fijos, mientras que, en otro modo de realización, estos parámetros se pueden enviar a la MS como parte de la BAKI. Mientras que la BAK se mantiene como secreto en el UIM 308, otros parámetros de la asociación de seguridad pueden mantenerse en el ME 306. En un modo de realización, en el que la SK se envía a la MS 300 como un paquete de IPSec cifrado usando BAK, el CS proporciona a los abonados un SPI usado para indexar la asociación de seguridad y este SPI se denomina SPLBAK.

**[0058]** El siguiente párrafo analiza cómo se actualiza la SK después de un proceso de abono exitoso. Dentro de cada período para actualizar la BAK, se proporciona un intervalo a corto plazo durante el cual la SK se distribuye en un canal de radiodifusión. El CS usa una función criptográfica para determinar dos valores SK y SKI (Información de SK) de modo que la SK pueda determinarse a partir de la BAK y la SKI. Por ejemplo, la SKI puede ser el cifrado de SK usando la BAK como clave. En un modo de realización ejemplar, la SKI es un paquete de IPSec en el que la carga útil contiene el valor de SK cifrado usando la BAK como clave. De forma alternativa, la SK puede ser el resultado de aplicar una función hash criptográfica a la concatenación de los bloques de SKI y BAK. El CS idealmente asegura que los valores de SK no se puedan predecir con antelación. Si se puede predecir la SK con antelación, a continuación, un atacante, es decir, una entidad de acceso ilegítima, puede enviar los valores pronosticados de SK a usuarios no abonados.

**[0059]** Como ejemplo, se supone que los valores de *N* de SK se usarán durante un período de 24 horas. Si se predice la SK con una precisión del 100 %, el atacante solo necesita pedir al UIM que calcule las *N* teclas. A continuación, el atacante pone las *N* teclas a disposición de los usuarios no abonados. Los usuarios no abonados pueden descargar las claves al comienzo de cada día y acceder al servicio de HSBS con poco coste o inconvenientes. Si el atacante solo puede predecir la SK con un 50 % de precisión, a continuación, el atacante debe enviar

aproximadamente *2N* claves. A medida que disminuye la exactitud de las predicciones, aumenta el número de claves que debe generar el atacante. Se puede disuadir a un atacante de distribuir las predicciones de SK asegurándose de que el coste de generar, almacenar y distribuir las predicciones exceda el beneficio de proporcionar el acceso ilegítimo. Los atacantes pueden desanimarse asegurando que la precisión de cualquier predicción del atacante sea lo suficientemente pequeña, aumentando por tanto el número de claves que generará el atacante hasta el punto en que el coste de proporcionar acceso ilegítimo exceda el beneficio. En consecuencia, cualquier esquema para generar SK idealmente asegura que las mejores predicciones de un atacante tengan una precisión suficientemente pequeña. Es decir, el cálculo de SK debe incluir algún valor aleatorio que solo se puede predecir con antelación con poca exactitud.

**[0060]** En un modo de realización ejemplar donde SK está en una forma cifrada, el CS puede seleccionar la SK usando una función aleatoria o pseudoaleatoria. En modos de realización alternativos, en los que la SK se deriva aplicando una función criptográfica a la SKI y la BAK, el CS introduce un valor impredecible al formar la SKI. Alguna parte de SKI puede ser predecible. Por ejemplo, una parte de SKI puede derivarse del tiempo del sistema durante el cual esta SKI es válida. Esta parte, denominada SKLPREDICT, no puede transmitirse a la MS 300 como parte del servicio de radiodifusión. El resto de SKI, SKLRANDOM puede ser impredecible. Es decir, SK_RANDOM se predice con poca exactitud. La SK_RANDOM se transmite a la MS 300 como parte del servicio de radiodifusión. La MS 300 reconstruye la SKI a partir de SKI_PREDICT y SKLRANDOM y proporciona la SKI al UIM 308. La SKI puede reconstruirse dentro del UIM 308. El valor de SKI cambia para cada nueva SK. Por tanto, la SKI_PREDICT y/o SKI_RANDOM cambian al calcular una nueva SK.

**[0061]** El CS envía la SKLRANDOM a la BS para la transmisión de radiodifusión. La BS transmite la SKI_RANDOM, que es detectada por la antena 302 y pasa a los circuitos de recepción 304. Los circuitos de recepción 304 proporcionan la SKLRANDOM a la MS 300, en los que la MS 300 reconstruye la SKI. La MS 300 proporciona la SKI al UIM 308, en el que el UIM 308 obtiene la SK usando la BAK almacenada en la SUMU 314. La SK es proporcionada a continuación por el UIM 308 al ME 306. El ME 306 almacena la SK en la unidad de almacenamiento de memoria, MEM 310. El ME 306 usa la SK para descifrar transmisiones de radiodifusión recibidas desde el CS.

**[0062]** El CS y la BS acuerdan algunos criterios sobre cuándo la SKI_RANDOM se va a transmitir. El CS puede desear reducir el valor monetario intrínseco en cada SK cambiando las SK con frecuencia. En esta situación, el deseo de cambiar los datos de SKI_RANDOM se equilibra con la optimización del ancho de banda disponible. En algunos modos de realización ejemplares, la SKI_RANDOM se envía con el contenido cifrado. Esto permite que la MS 300 genere la SK y comience a descifrar de inmediato. En muchas situaciones, esto desperdiciará el ancho de banda. Una excepción es un esquema en el que la SKLRANDOM se envía como parámetros de la comunicación. Por ejemplo, el valor de SPI en IPSec puede variar y puede explotarse para incluir un valor de SKLRANDOM, como se analiza con más detalle a continuación en el presente documento.

**[0063]** En otros modos de realización, la SKLRANDOM se envía por separado desde el contenido cifrado. La SKI_RANDOM puede incluso transmitirse en un canal que no sea el canal de radiodifusión. Cuando un usuario "sintoniza" el canal de radiodifusión, los circuitos de recepción 304 obtienen información para localizar el canal de radiodifusión desde un "canal de control". Puede ser deseable permitir un acceso rápido cuando un usuario "sintoniza" el canal de radiodifusión. Esto requiere que el ME 306 obtenga SKI en un corto período de tiempo. Es posible que el ME 306 ya conozca la SKI_PREDICT, sin embargo, la BS proporciona la SKLRANDOM al ME 300 dentro de este corto período de tiempo. Por ejemplo, la BS puede transmitir con frecuencia SKLRANDOM en el canal de control, junto con la información para localizar el canal de radiodifusión, o transmitir con frecuencia SKI_RANDOM en el canal de radiodifusión. Cuanto más a menudo la BS "actualiza" el valor de SKI_RANDOM, más rápido la MS 300 puede acceder al mensaje de radiodifusión. El deseo de actualizar los datos de SKI_RANDOM se equilibra con la optimización del ancho de banda disponible, ya que la transmisión de datos de SKI_RANDOM con demasiada frecuencia puede usar una cantidad inaceptable de ancho de banda en el canal de control o en el canal de radiodifusión.

**[0064]** En algunas situaciones, el CS puede optar por usar valores de SKI_PREDICT y SKLRANDOM en el que ambos cambian para cada valor de SK producido. En otras situaciones, el CS puede desear reducir el número de veces que la SKLRANDOM cambia, de modo que la MS 300 no tenga que obtener la SKI_RANDOM con tanta frecuencia. Por ejemplo, si un usuario cambia con frecuencia entre múltiples canales de HSBS, sería mejor que el valor de SKI_RANDOM no cambiara en los cinco minutos durante los cuales el usuario está sintonizado en otro canal. Si la SKI_RANDOM cambiara, el usuario tendría que esperar a continuación hasta que se emita el nuevo valor de SKI_RANDOM, lo que indica que dicho esquema sería más "fácil de usar" si la SKI_RANDOM permanece constante durante el mayor tiempo posible. El CS puede desear usar múltiples valores de SK durante la vida útil de un valor de SKLRANDOM, usando un valor para SKI_PREDICT que habrá cambiado cada vez que el CS desee cambiar la SK. Un ejemplo usa la hora del sistema; sin embargo, el uso de la hora del sistema presenta problemas adicionales con respecto a la sincronización.

**[0065]** Con respecto al cifrado y la transmisión del contenido de radiodifusión, el CS cifra el contenido de radiodifusión usando la SK actual. El modo de realización ejemplar emplea un algoritmo de cifrado tal como el Algoritmo de cifrado del Estándar de cifrado avanzado (AES). En el modo de realización ejemplar, el contenido cifrado a continuación es transportado por un paquete de IPsec de acuerdo con el modo de transporte de carga útil de seguridad de encapsulado (ESP) analizado a continuación en el presente documento. El paquete de IPsec también

contiene un valor de SPI que ordena al ME 306 que use la SK actual para descifrar el contenido de radiodifusión recibido. El contenido cifrado se envía por medio del canal de radiodifusión.

**[0066]** Los circuitos de recepción 304 proporcionan la RKI y la BAKI directamente al UIM 308. Además, si el CS calcula la SK a partir de valores de SKI_RANDOM y SKI_PREDICT, los circuitos de recepción 304 proporcionan a continuación la SKI_RANDOM a una parte apropiada de la MS 300 donde se combina con SKI_PREDICT para obtener SKI. En un modo de realización, la SKI se adjunta al mensaje cifrado y el ME 306 lo extrae. La parte relevante de la MS 300 proporciona la SKI al UIM 308. El UIM 308 calcula la RK a partir de la clave RKI y A, descifra la BAKI usando la RK para obtener la BAK, y calcula la SK usando la SKI y la BAK, para generar una SK para su uso por el ME 306. El ME 306 descifra el contenido de radiodifusión usando la SK. El UIM 308 del modo de realización ejemplar puede no ser lo suficientemente potente para descifrar el contenido de radiodifusión en tiempo real y, por lo tanto, la SK se transfiere al ME 306 para descifrar la radiodifusión.

**[0067]** Las FIGS. 5A y 5B ilustran la transmisión y el procesamiento de claves, que incluyen RK, BAK y SK, de acuerdo con un modo de realización ejemplar. Como se ilustra, en el registro, la MS 300 recibe la información de RK (RKI) y la transmite al UIM 308, en el que la SUPU 316 calcula la RK usando la RKI y la tecla A, y almacena la RK en el almacenamiento de memoria de UIM SUMU 314. La MS 300 recibe periódicamente la información de BAK (BAKI) que contiene la BAK cifrada usando el valor de RK específico de UIM 308. La BAKI cifrada es descifrada por la SUPU 316 para recuperar la BAK, que se almacena en el almacenamiento de memoria de UIM SUMU 314. La MS 300 obtiene además periódicamente la SKI. En algunos modos de realización ejemplares, la MS 300 recibe una SKI_RANDOM que combina con SKI_PREDICT para formar la SKI. La SUPU 316 calcula la SK a partir de SKI y BAK. La SK se proporciona al ME 306 para descifrar el contenido de radiodifusión.

**[0068]** En el modo de realización ejemplar, las claves de CS no se cifran y transmiten necesariamente a la MS; el CS puede usar un procedimiento alternativo. La información clave generada por el CS para su transmisión a cada MS proporciona información suficiente para que la MS calcule la clave. Como se ilustra en el sistema 350 de la FIG. 6, la RK es generada por el CS, pero la información de RK (RKI) se transmite a la MS. El CS envía información suficiente para que el UIM derive la RK, en el que se usa una función predeterminada para derivar la RK a partir de la información transmitida desde el CS. La RKI contiene información suficiente para que la MS determine la RK original a partir de la tecla A y otros valores, tal como la hora del sistema, usando una función pública predeterminada etiquetada como d1, en la que:

$$RK = d1(\text{clave A}, RKI). \quad (3)$$

**[0069]** En el modo de realización ejemplar, la función d1 define una función de tipo criptográfico. De acuerdo con un modo de realización, la RK se determina como:

$$RK = SHA'(\text{clave A} \parallel RKI), \quad (4)$$

en la que "||" indica la concatenación de los bloques que contienen la tecla A y RKI, y SHA '(X) indica los últimos 128 bits de salida del algoritmo hash seguro SHA-1 dada la entrada X. En un modo de realización alternativo, RK se determina como:

$$RK = AES(\text{clave A}, RKI), \quad (5)$$

en la que AES (X, Y) indica el cifrado de la RKI de bloque de 128 bits usando la clave A de 128 bits. En un modo de realización adicional basado en el protocolo de AKA, la RK se determina como la salida de la función de generación de clave de 3GPP *f3,* en la que la RKI incluye el valor de RAND y los valores apropiados de AMF y SQN como se define por el estándar.

**[0070]** La BAK se trata de manera diferente porque múltiples usuarios que tienen diferentes valores de RK deben calcular el mismo valor de BAK. El CS puede usar cualquier técnica para determinar la BAK. Sin embargo, el valor de BAKI asociado con un UIM 308 particular debe ser el cifrado de BAK bajo la RK única asociada con ese UIM 308. La SUPU 316 descifra la BAKI usando la RK almacenada en la SUMU 314 de acuerdo con la función etiquetada como d2, de acuerdo con:

$$BAK = d2(BAKI, RK). \quad (6)$$

**[0071]** En un modo de realización alternativo, el CS puede calcular la BAKI aplicando un proceso de descifrado a la BAK usando la RK, y la SUPU 316 obtiene la BAK aplicando el proceso de cifrado a la BAKI usando la RK. Esto se considera equivalente al CS que cifra la BAK y a la SUPU 316 que descifra la BAKI. Los modos de realización alternativos pueden implementar cualquier número de combinaciones de claves además de o en lugar de las ilustradas en la FIG. 6.

**[0072]** La SK se trata de forma similar a la RK. En algunos modos de realización, la SKI se deriva primero de SKI_PREDICT y SKI_RANDOM, en los que 9KI_RANDOM es la información transmitida desde el CS a la MS. A continuación, se usa una función predeterminada etiquetada como d3 para derivar la SK desde SKI y BAK (almacenada en la SUMU 314), de acuerdo con:

$$SK = d3(BAK, SKI). \quad (7)$$

**[0073]** En un modo de realización, la función d3 define una función de tipo criptográfico. En un modo de realización ejemplar, la SK se calcula como:

$$SK = SHA( BAK \,||\, SKI ), \quad (8)$$

mientras que, en otro modo de realización, la SK se calcula como

$$SK = AES( BAK, SKI ). \quad (9)$$

**[0074]** Un procedimiento de proporcionar la seguridad para un mensaje de radiodifusión se ilustra en las FIGS. 7A-7D. La FIG. 7A ilustra un proceso de registro 400 en el que un abonado negocia el registro con el CS en la etapa 402. El registro en la etapa 404 proporciona al UIM una RK única. El UIM almacena la RK en una unidad de memoria segura (SUMU) en la etapa 406. La FIG. 7B ilustra el procesamiento de abono 420 entre un CS y una MS. En la etapa 422, el CS genera una BAK durante un período de tiempo de BAK T1. La BAK es válida durante todo el período de tiempo de BAK T1, en el que la BAK se actualiza periódicamente. En la etapa 424, el CS autoriza al UIM a tener acceso al contenido de radiodifusión (BC) durante el período del temporizador de BAK T1. En la etapa 426, el CS cifra la BAK usando cada RK individual para cada abonado. La BAK cifrada se denomina BAKI. A continuación, el CS transmite la BAKI al UIM en la etapa 428. El UIM recibe la BAKI y realiza el descifrado usando la RK en la etapa 430. La BAKI descifrada da como resultado la BAK generada originalmente. El UIM almacena la BAK en una SUMU en la etapa 432.

**[0075]** Cuando el usuario se abona al servicio de radiodifusión durante un período de actualización de BAK particular, el CS envía la información apropiada BAKI, en el que la BAKI corresponde a la BAK cifrada con la RK. Esto se produce típicamente antes del comienzo de este período de actualización de BAK o cuando la MS sintoniza por primera vez el canal de radiodifusión durante este período de actualización de BAK. Este puede ser iniciado por la MS o el CS de acuerdo con una variedad de criterios. Se pueden transmitir y descifrar múltiples BAKI simultáneamente.

**[0076]** Debe observarse que cuando la caducidad del período de actualización de BAK es inminente, la MS puede solicitar la BAK actualizada del CS si la MS se ha abonado para el próximo período de actualización de BAK. En un modo de realización alternativo, el CS usa el primer temporizador t1, donde al caducar el temporizador, es decir, cuando se cumple el período de actualización de BAK, el CS transmite la BAK. El CS puede cambiar el valor de BAK antes de lo previsto originalmente. Esto puede ser deseable si, por ejemplo, el valor actual de BAK se divulga públicamente.

**[0077]** Debe observarse que es posible que un usuario reciba una BAK durante un período de actualización de BAK, en el que, por ejemplo, un abonado se une al servicio a mediados de mes cuando las actualizaciones de BAK se realizan mensualmente. Adicionalmente, los períodos de tiempo para las actualizaciones de BAK y SK pueden sincronizarse, de modo que todos los abonados se actualicen en un momento dado.

**[0078]** La FIG. 8A ilustra el proceso de registro en un sistema de comunicación inalámbrica 500 de acuerdo con el modo de realización ejemplar. El CS 502 negocia con cada abonado, es decir, MS 512, para generar una RK específica para cada uno de los abonados. La RK se proporciona a la unidad SUMU dentro del UIM de cada MS. Como se ilustra, el CS 502 genera $RK_1$ que se almacena en $SUMU_1$ 510 dentro de $UIM_1$ 512. De forma similar, el CS 502 genera $RK_2$ y $RK_N$ que se almacenan en $SUMU_2$ 520 dentro de $UIM_2$ 522 y $SUMU_N$ 530 dentro de $UIM_N$ 532, respectivamente.

**[0079]** La FIG. 8B ilustra el proceso de abono en el sistema 500. El CS 502 incluye además múltiples codificadores 504. Cada uno de los codificadores 504 recibe una de las RK únicas y el valor de BAK generado en el CS 502. La salida de cada codificador 504 es una BAKI codificada específicamente para un abonado. La BAKI se recibe en el UIM de cada MS, tal como $UIM_1$ 512. Cada UIM incluye una SUPU y una SUMU, tal como $SUPU_1$ 514 y $SUMU_1$ 510 de $UIM_1$ 512 y $SUPU_N$ 534 y $SOMU_N$ 530 de $UIM_N$ 532. La SUPU incluye un descodificador, tal como el descodificador 516 o el descodificador 536 que recupera la BAK mediante la aplicación de la RK del UIM. El proceso se repite en cada abonado.

**[0080]** La FIG. 8D ilustra el procesamiento de BC después del registro y abono. El CS 502 incluye un codificador 560 que codifica el BC usando la SK actual para generar el EBC. El EBC se transmite a continuación a los abonados.

Cada MS incluye un codificador, tal como el codificador 544 o el codificador 554, que extrae el BC del EBC usando la SK.

**[0081]** La siguiente descripción considera cuatro modos de realización ejemplares que pueden usarse para actualizar la SK y difundir el contenido. En el primer modo de realización ejemplar, la SK se deriva de BAK y el valor de SPI en la cabecera de los paquetes de IPSec que contienen el contenido de radiodifusión. En el segundo modo de realización ejemplar, la SK se deriva de BAK, un valor aleatorio de radiodifusión denominado RAND y el valor de SPI en la cabecera de los paquetes de IPSec que contienen el contenido de radiodifusión. En el tercer modo de realización ejemplar, la SK se deriva de BAK, la hora del sistema y un valor aleatorio de radiodifusión denominado SK_RAND. En el cuarto modo de realización ejemplar, la SK se envía como un paquete de IPSec cifrado usando la BAK. Otros modos de realización más pueden proporcionar la SK como una combinación de los modos de realización enumerados anteriormente, o usar otro mecanismo para proporcionar la SK a la MS con la frecuencia suficiente para desalentar el acceso no autorizado al servicio de radiodifusión.

**[0082]** Como la clave a corto plazo (SK) se usa para cifrar y descifrar el contenido de radiodifusión, y se almacena en la memoria que puede ser vulnerable al acceso no autorizado, en la que la SK típicamente se cambia con frecuencia, existe un problema sobre cómo cambiar la SK con frecuencia mientras se equilibran los siguientes cuatro objetivos: 1) minimizar el tiempo de espera de actualización de SK o el período de prohibición, para una estación móvil que recientemente ha sintonizado la radiodifusión; 2) minimizar la cantidad de ancho de banda usada para actualizar el valor de SK; 3) aumentar el nivel de seguridad; y 4) aumentar la facilidad con la que se puede incorporar la SK con IPSec. Las actualizaciones frecuentes pueden reducir el período de prohibición, pero a expensas de requerir más ancho de banda para enviar actualizaciones frecuentes.

**[0083]** Una solución proporciona un procedimiento para proporcionar información suficiente para realizar actualizaciones de SK en cada paquete de contenido de radiodifusión cifrado sin usar ningún ancho de banda adicional. Por lo tanto, el período de prohibición puede minimizarse sin incurrir necesariamente en requisitos de ancho de banda adicionales. Los cuatro modos de realización ejemplares descritos en el presente documento para realizar una actualización de SK tienen diversas ventajas y desventajas. Los cuatro modos de realización proporcionan procedimientos que son suficientemente seguros. El primer modo de realización elimina el período de prohibición y no usa ancho de banda adicional para actualizar el valor de SK. Los otros modos de realización pueden incurrir en un período de prohibición durante periodos de alto uso. El primer modo de realización también se incorpora fácilmente con IPSec.

**[0084]** De acuerdo con el primer modo de realización para realizar una actualización de SK, los problemas mencionados anteriormente se resuelven definiendo la SK que cifra un paquete de IRSec dado en función de la Clave de acceso de radiodifusión (BAK) y el SPI en la cabecera de ESP. De esta manera, en lugar de proporcionar la SK en una secuencia separada, la SK se calcula a partir de la secuencia de contenido. Suponiendo que la MS ya ha recibido la BAK como se describe anteriormente en el presente documento, la MS puede calcular de inmediato la SK para cada paquete de contenido sin tener que esperar alguna información adicional de actualización de la SK. Esto elimina eficazmente cualquier tiempo de espera de actualización de SK para un nuevo destinatario de radiodifusión. Tan pronto como la MS recibe un paquete de contenido, la MS puede determinar de inmediato la SK y descifrar el contenido.

**[0085]** La información suficiente para calcular la SK en la MS se proporciona en el paquete de IPSec. El paquete de IPSec utiliza una carga útil de seguridad de encapsulación de IP (ESP) y se especifica en RFC 1827 titulado "IP Encapsulating Security Payload (ESP)" por R. Atkinson en agosto de 1995, como se menciona anteriormente en el presente documento. La ESP es un mecanismo para proporcionar integridad y confidencialidad a los datagramas de IP. En algunas circunstancias, también puede proporcionar autenticación a datagramas de IP. La FIG. 9A ilustra un paquete de IPSec 600, que incluye una cabecera de IP 602, una cabecera de ESP 604 y una carga útil 606, de acuerdo con un modo de realización. La carga útil de seguridad de encapsulación (ESP) puede aparecer en cualquier lugar después de la cabecera de IP y antes del protocolo final de la capa de transporte. En general, la ESP consiste en una cabecera sin cifrar seguido de datos cifrados.

**[0086]** El campo de cabecera de ESP 604 incluye un identificador de asociación de seguridad, denominado SPI. De acuerdo con el primer modo de realización descrito anteriormente en el presente documento, los paquetes de IPSec que contienen el contenido de radiodifusión incluyen un SPI relacionado con la SK, etiquetado como SPI_SK. La FIG. 9B ilustra el formato del correspondiente SPI_SK de 32 bits 610. El SPI_SK 610 se descompone en dos partes: SPI_RAND 612 y BAK_ID 614. El SPI_RAND 612 es un número aleatorio que es estadísticamente aleatorio y también se usa para calcular la SK que se usa para cifrar y descifrar el contenido de radiodifusión o carga útil correspondiente. El parámetro SPI_RAND permite que el servidor de contenido (CS) cambie con frecuencia el valor efectivo de SK para el contenido cambiando el valor de SPLRAND, proporcionando por tanto a la MS el parámetro necesario para calcular el valor de SK de inmediato. Además, SPI_RAND cumple el papel de SKLRANDOM, analizado anteriormente en el presente documento. La aleatoriedad de SPI_RAND asegura que un atacante no pueda predecir los valores de SK con alta precisión. Dado que el SPI ya es un parámetro estándar en los paquetes cifrados de IPSec, es decir, se especifica para la ESP, el presente modo de realización no incurre en el ancho de banda adicional típicamente asociado con la transmisión de la SK como una secuencia separada. El BAK_ID indica qué valor de BAK usar para el cálculo del valor de SK. En un modo de realización, el BAK_ID es una etiqueta de cuatro bits, en el que cada etiqueta

está asociada con un valor de BAK. Cuando la MS realiza un abono, la MS almacena cada BAK_ID recibido y el valor de BAK correspondiente en una unidad de almacenamiento de memoria. De acuerdo con un modo de realización, la MS incluye una tabla de búsqueda (LUT) para almacenar el (los) valor(es) de BAK identificado(s) con cada BAK_ID correspondiente. La LUT de BAK está contenida en la memoria segura en el UIM.

**[0087]** La FIG. 9D ilustra una LUT de BAK 630. Cada entrada en la LUT 630 identifica el BAK_ID, el valor de BAK correspondiente y la caducidad de la validez de la combinación. La caducidad se introduce debido al pequeño número de valores de BAK_ID. Los modos de realización alternativos pueden evitar el uso de valores de caducidad en la LUT de BAK. En un modo de realización, solo se usan 16 valores de BAK_ID. Si se emite una nueva BAK todos los meses, el valor de BAK_ID debe repetirse después de 16 meses. En ese momento, puede haber confusión sobre qué valor de BAK es válido. La caducidad proporciona un período de tiempo de espera después del cual una nueva entrada reemplaza la entrada caducada. La LUT de BAK puede necesitar almacenar más de un valor de BAK. Un motivo para esto es que el CS puede desear enviar valores de BAK a la MS antes de que resulten válidos. Además, el CS puede desear tener múltiples valores de BAK que sean válidos al mismo tiempo, en el que se pueden usar diferentes valores de BAK para calcular diferentes valores de SK. Si la LUT de BAK no contiene una BAK actual correspondiente al BAK_ID, entonces la MS puede realizar una suscripción para recuperar la BAK válida.

**[0088]** Después de extraer SPLRAND y BAK_ID del SPI_SK, y recuperar la BAK correspondiente al BAK_ID, el UIM calcula el valor de SK de BAK y SPI_RAND usando una función criptográfica *g*:

$$SK = g(BAK, SPI\_RAND). \quad (10)$$

**[0089]** En un modo de realización, la función g(BAK, SPLRAND) corresponde al cifrado de SPI_RAND relleno con bits de 128 bits con ceros, usando el algoritmo de cifrado AES con BAK como clave:

$$SK = AES(BAK, SPI\_RAND). \quad (11)$$

**[0090]** En otro modo de realización, la función g(BAK, SPLRAND) corresponde al cálculo de los 128 bits menos significativos de la salida de SHA-1 aplicados a la concatenación de BAK y SPLRAND:

$$SK = SHA(BAK, SPI\_RAND). \quad (12)$$

**[0091]** De esta manera, no es necesario que el UIM calcule el valor de SK para cada paquete recibido por la MS. La MS almacena cada uno de los valores de SPI_SK con los valores de SK correspondientes en una unidad de almacenamiento de memoria, tal como una tabla de búsqueda (LUT). La MS puede almacenar los valores de SPI_SK y SK como una asociación de seguridad en la base de datos de asociación de seguridad (SAD): una LUT en la que la MS almacena asociaciones de seguridad típicas requeridas para otras aplicaciones. Las asociaciones de seguridad se indexan de acuerdo con la dirección de destino y el SPI. Cuando se genera una nueva SK a partir de un nuevo valor de SPI_SK, la antigua asociación de seguridad se reemplaza por la nueva asociación de seguridad que contiene los nuevos valores de SPI_SK y SK. De forma alternativa, la MS puede almacenar los valores de SPI_SK y SK en una SK_LUT, con una SK_LUT asignada a cada canal de radiodifusión. La FIG. 9C ilustra una LUT de SK 620. Cada entrada en la LUT 620 identifica la SPI_SK y el valor de SK correspondiente. Cuando la MS recibe un paquete de contenido de radiodifusión, el ME primero verifica la SAD o LUT de SK para ver si la tabla contiene un valor de SPI_SK igual al SPI del paquete recibido. Si la tabla contiene dicho valor, el ME usa este valor, de lo contrario, el UIM calcula el nuevo valor de SK. El CS también puede tener una LUT de BAK, SAD o SK_LUT.

**[0092]** Las FIGS. 10 y 11 ilustran un modo de realización para realizar una actualización de SK. La FIG. 10 ilustra el procedimiento de funcionamiento 700 del CS. Para cada paquete IP, el CS determina la BAK que se usará para derivar la SK, y determina el BAK_ID correspondiente a la BAK en la etapa 702. El BAK_ID puede ser cualquier tipo de identificador que permita la discriminación entre múltiples valores de BAK. El CS envía la BAK y el BAK_ID a usuarios individuales mediante el abono en la etapa 706. Los usuarios pueden realizar abonos en varios momentos antes y durante el período de abono. Las etapas 702 y 706 pueden tener lugar antes de que comience el período de abono. En la etapa 710, el CS selecciona un valor aleatorio para el valor SPI_RAND. Si el BAK_ID se representa usando *b* bits, entonces el SPI_RAND se representa usando (32-*b*) bits. El valor SPI_RAND no debe repetirse durante la vida útil de una BAK. Una vez que se conocen SPLRAND y BAK_ID, el CS los combina (es decir, concatena BAK_ID con SPLRAND) para formar SPI_SK en la etapa 712. En la etapa 714, el CS forma la SK usando una función criptográfica para combinar SPI_RAND con la BAK correspondiente al BAK_ID para formar la SK. A continuación, el CS cifra el mensaje de radiodifusión o parte del mensaje con la SK en la etapa 716, y envía el mensaje cifrado en la etapa 718. Debe observarse que el mensaje de radiodifusión cifrado es parte de un paquete IP que incluye la cabecera IP y la cabecera ESP. La cabecera ESP incluye el SPI_SK. En el rombo de decisión 720, el CS decide si cambiar la SK. Si el CS decide no cambiar la SK, entonces el CS continúa con la etapa 716. Si el CS decide cambiar la SK, entonces el CS continúa con el rombo de decisión 724, donde el CS decide si cambiar la BAK. Si el CS decide no cambiar la BAK, entonces el CS continúa con la etapa 710. Si el CS decide cambiar la BAK, entonces el CS continúa con la etapa 702.

**[0093]** La FIG. 11 ilustra la operación correspondiente en el receptor, tal como una MS. El procedimiento 750 se inicia cuando el receptor recibe el paquete IP que incluye el SPI_SK en la cabecera ESP en la etapa 752. Debe observarse que el receptor extrae la información de SPI_SK del paquete IP. Al recibir el SPI_SK, el receptor primero verifica si la SK correspondiente al valor de SPI_SK recibido está almacenado en la memoria.

**[0094]** En un modo de realización, el SPI_SK se almacena en una LUT de SK almacenada en la unidad de ME 306 de la FIG. 4 y en otro modo de realización, el SPI_SK se almacena en la base de datos de asociación de seguridad: ambas tablas se indican en la FIG. 11 mediante la tabla de SPI. La verificación de la tabla de SPI se realiza en el rombo de decisión 754. Si el valor de SK se almacena en memoria en el receptor, el receptor puede descifrar la carga útil del paquete de contenido usando el valor de SK almacenado en la etapa 756. Si el receptor no tiene el valor de SK almacenado en memoria, el receptor extrae el BAK_ID y SPI_RAND desde el SPI_SK en la etapa 758. En la etapa 760, el receptor verifica a continuación si la LUT de BAK tiene una entrada de BAK válida correspondiente al BAK_ID. Si la LUT de BAK sí tiene una BAK válida correspondiente al BAK_ID, entonces el receptor selecciona este valor y continúa con la etapa 764. Si la LUT de BAK no tiene una BAK válida correspondiente al BAK_ID, tal como cuando el usuario desea abonarse para este período, entonces el receptor realiza un abono para obtener la BAK válida como se muestra en la etapa 762. La nueva BAK se almacena con BAK_ID en la BAK_LUT y el receptor continúa con la etapa 764. El receptor combina la BAK correspondiente al valor de BAK_ID, es decir, el BAK_ID en el SPI_SK recibido, y el valor de SPLRAND (también en el SPI_SK recibido) para calcular la nueva SK en la etapa 764. A continuación, el receptor usa el nuevo valor de SK para descifrar la carga útil del paquete de contenido en la etapa 766. El receptor también almacena este valor de SK indexado por el SPI_SK correspondiente y posiblemente la dirección de destino de los paquetes de IPSec.

**[0095]** La SK se calcula directamente a partir del conocimiento de la BAK y el valor de SPI_SK en el paquete de contenido. La BAK cambia con menos frecuencia que la SK, por ejemplo, la BAK puede cambiar una vez al mes. Por lo tanto, el receptor puede determinar el valor de SK de inmediato a partir de los paquetes de contenido sin demora adicional y sin requerir más ancho de banda para enviar la actualización de SK.

**[0096]** De acuerdo con un modo de realización, el cálculo de SK se da como:

$$SK=f(SPI\_SK, BAK), \qquad (13)$$

en el que la función se define como el cifrado del SPI_SK usando la BAK. Como el SPI_SK está compuesto de SPI_RAND y BAK_ID, la ecuación (13) también se puede dar como:

$$SK=f(SPI\_RAND, BAK\_ID). \qquad (14)$$

**[0097]** El segundo modo de realización ejemplar para realizar una actualización de SK introduce un aspecto adicional de aleatoriedad para el cálculo de SK, en el que SK se define como una función de BAK, SPI_RAND y un parámetro adicional, RAND. El parámetro RAND se mantiene constante para varios valores de SK. El RAND permite que se obtengan más valores diferentes de SK a partir de un solo valor de BAK cambiando SPI_RAND y RAND. Si no se usa RAND, entonces existen como máximo $2^{32}$ valores de SK que pueden derivarse de una sola BAK variando el SPI. Sin embargo, si se usa un RAND de 96 bits, puede haber entonces hasta $2^{218}$ valores de SK que se pueden derivar de una sola BAK variando SPI_RAND y RAND. (Estos números no tienen en cuenta los bits del SPI que se usan para representar el BAK_ID). Ahora, en lugar de que SPI_SK identifique solo la BAK, SPI_SK también debe contener información para identificar el RAND. Para implementar el valor de RAND, el SPI_SK se formula en tres partes: 1) el BAK_ID para identificar el valor de BAK que se va a usar; 2) el RAND_ID para identificar el valor de RAND que se va a usar; y 3) el valor de SPI_RAND para proporcionar la aleatoriedad que cambia con frecuencia en el SPI_SK.

**[0098]** La FIG. 12A ilustra una parte de SPI_SK 800 de un paquete IP, que incluye un SPI_RAND 802, un BAK_ID 804 y un RAND_ID 806. El SPI_RAND 802 y el BAK_ID 804 son como se describe anteriormente en el presente documento. Para mantener el SPI_SK a una longitud de bit predeterminada o especificada, el SPI_RAND 802 puede usar menos bits que el SPI_RAND 612 como en la FIG. 9B para permitir bits para el RAND_ID 806. El RAND_ID 806 corresponde al valor de RAND usado para el cálculo de la SK, y puede ser una etiqueta de cuatro bits u otro identificador. El (los) RAND_ID y el (los) valor(es) de RAND correspondiente(s) se almacenan en una LUT en el receptor. La FIG. 12B ilustra una LUT de RAND 820. La LUT de RAND 820 incluye una entrada para cada valor de RAND que enumera el RAND_ID y la caducidad asociada con el valor de RAND.

**[0099]** La FIG. 13 ilustra la operación 900 del CS. Para cada paquete IP, el transmisor determina la BAK que se usará para derivar la SK, y determina el BAK_ID correspondiente a la BAK en la etapa 902. El BAK_ID puede ser cualquier tipo de identificador que permita la discriminación entre múltiples valores de BAK. El CS envía la BAK y el BAK_ID a usuarios individuales mediante el abono en la etapa 904. Los usuarios pueden realizar abonos en varios momentos antes y durante el período de abono. Las etapas 902 y 904 pueden tener lugar antes de que comience el período de abono. En la etapa 906, el transmisor selecciona un valor de RAND y determina el RAND_ID correspondiente. En la etapa 908, el CS puede enviar el RAND y el RAND_ID a la MS individualmente o enviar el RAND y el RAND_ID para su radiodifusión en el canal de radiodifusión. El valor de RAND no necesita ser secreto, por

lo que no está cifrado. Si se radiodifunde el RAND y el RAND_ID, entonces no debería haber mucho tiempo entre la retransmisión de modo que una MS no necesite esperar mucho antes de obtener el valor de RAND. La radiodifusión de RAND y RAND_ID usará una gran cantidad de ancho de banda a lo largo del tiempo. Sin embargo, si hay una gran cantidad de usuarios sintonizados en el canal, entonces se requerirá una gran cantidad de ancho de banda para enviar RAND a cada usuario individualmente. En consecuencia, RAND y RAND_ID solo deben radiodifundirse si hay una gran cantidad de usuarios sintonizados en el canal. En la etapa 910, el CS selecciona un valor aleatorio de SPLRAND.

**[0100]** Una vez que se conocen SPLRAND, BAK_ID y RAND_ID, el transmisor los combina (por ejemplo, concatena RAND_ID y BAK_ID con el SPLRAND) para formar el SPI_SK en la etapa 912. El CS usa una función criptográfica para combinar SPI_RAND, BAK (identificada por el BAK_ID) y RAND (identificado por el RAND_ID) para formar la SK en 914. A continuación, el CS cifra el mensaje de radiodifusión o parte del mensaje con SK en la etapa 916, y transmite el mensaje cifrado en la etapa 918. Debe observarse que el mensaje de radiodifusión cifrado es parte de un paquete IP que incluye la cabecera IP y la cabecera ESP. La cabecera ESP incluye el SPI_SK. En el rombo de decisión 920, el CS decide si cambiar la SK. Si el CS decide no cambiar la SK, entonces el CS continúa con la etapa 916. Si el CS decide cambiar la SK, entonces el CS continúa con el rombo de decisión 922, donde el CS decide si cambiar el RAND. Si el CS decide no cambiar el RAND, entonces el CS continúa con la etapa 910. Si el CS decide cambiar el RAND, entonces el CS continúa con el rombo de decisión 924, donde el CS decide si cambiar la BAK. Si el CS decide no cambiar la BAK, entonces el CS continúa con la etapa 906. Si el CS decide cambiar la BAK, entonces el CS regresa a la etapa 902.

**[0101]** La FIG. 14 ilustra la operación correspondiente en el receptor, tal como una MS. El procedimiento 950 se inicia cuando el receptor recibe el paquete IP que incluye el SPI_SK en la cabecera ESP en la etapa 952. Debe observarse que el receptor extrae la información de SPI_SK del paquete IP. Al recibir el SPI_SK, el receptor primero verifica si la SK correspondiente al valor de SPI_SK recibido está almacenado en la memoria en el rombo de decisión 952. En un modo de realización, el SPI_SK se almacena en una LUT de SK almacenada en la unidad de ME 306 de la FIG. 4 y en otro modo de realización, el SPI_SK se almacena en la base de datos de asociación de seguridad: ambas tablas se indican en la FIG. 14 como la tabla de SPI. La verificación de la LUT de SK se realiza en el rombo de decisión 954. Si el valor de SK se almacena en memoria en el receptor, el receptor puede descifrar la carga útil del paquete de contenido usando el valor de SK almacenado en la etapa 956. Si el receptor no tiene el valor de SK almacenado en memoria, el receptor extrae el BAK_ID y SPI_RAND desde el SPI_SK en la etapa 958. En la etapa 960, el receptor verifica a continuación si la LUT de BAK tiene una entrada de BAK válida correspondiente al BAK_ID. Si la LUT de BAK sí tiene un RAND válido correspondiente al BAK_ID, entonces el receptor selecciona este valor y continúa con la etapa 964. Si la LUT de BAK no tiene una BAK válida correspondiente al BAK_ID, entonces (suponiendo que el usuario desee abonarse para este período), el receptor realiza un abono para obtener la BAK válida como se muestra en la etapa 962. La nueva BAK se almacena con BAK_ID en la BAK_LUT y el receptor continúa con la etapa 864. En la etapa 964, el receptor verifica a continuación si la LUT de RAND tiene una entrada de RAND válida correspondiente al RANK_ID. Si la LUT de BAK sí tiene una BAK válida correspondiente al RAND_ID, entonces el receptor selecciona este valor y continúa con la etapa 964. Si la LUT de RAND no tiene una RAND válida correspondiente al RAND_ID, entonces el receptor obtiene el RAND y el RAND_ID solicitando el valor tanto desde el CS como desde la radiodifusión como se muestra en la etapa 966. El nuevo RAND se almacena con el RAND_ID en la RAND_LUT y el receptor continúa con la etapa 968. El receptor combina la BAK correspondiente al valor de BAK_ID (es decir, BAK_ID en el SPI_SK recibido), el RAND correspondiente al RAND_ID (es decir, RAND_ID en el SPI_SK recibido) y el valor de SPI_RAND (también en el SPI_SK recibido) para calcular la nueva SK en la etapa 968. A continuación, el receptor usa el nuevo valor de SK para descifrar la carga útil del paquete de contenido en la etapa 970. El receptor también almacena este valor de SK indexado por el SPI_SK correspondiente y posiblemente la dirección de destino de los paquetes de IPSec.

**[0102]** El RAND se cambia con menos frecuencia que el SPI_RAND. El valor de RAND es común a todas las estaciones móviles que escuchan la radiodifusión. Por lo tanto, el valor de RAND puede radiodifundirse a todas las estaciones móviles y no está necesariamente cifrado específicamente por receptor. Por lo tanto, si hay suficientes estaciones móviles que escuchan la transmisión por radiodifusión, es más eficaz que la interfaz aérea radiodifunda el valor de RAND varias veces a todas estas estaciones móviles en lugar de requerir que cada estación móvil solicite individualmente los valores de RAND del CS.

**[0103]** De acuerdo con un modo de realización, el cálculo de SK se da como:

$$SK=f(SPI\_SK, BAK, RAND), \quad (15)$$

en el que la función se define como el cifrado del SPI_SK usando la BAK. Como el SPI_SK está compuesto del SPLRAND, el BAK_ID y el RAND_ID, la ecuación (15) también se puede dar como:

$$SK=f(SPI\_RAND, BAK\_ID, RAND\_ID, RAND). \quad (16)$$

**[0104]** Debe observarse que el uso de un valor de RAND puede introducir algunos "períodos de prohibición" porque el receptor necesita recibir el valor de RAND en un cambio. Sin embargo, estos períodos son menos frecuentes que cuando la SK se actualiza en una secuencia separada y el receptor espera las actualizaciones periódicas. El RAND está diseñado para cambiar más lentamente que el valor de SK y, por lo tanto, las actualizaciones de RAND no se envían con tanta frecuencia. El CS también desea reducir la probabilidad de una "prohibición" resultante cuando una MS deja de escuchar el canal debido a una señal perdida, sintonizando otro canal o respondiendo a una interrupción, tal como una llamada telefónica. La prohibición es más probable que se produzca al comienzo de la vida útil de un valor de RAND. Para contrarrestar esto, el CS puede retransmitir por radiodifusión el nuevo RAND con más frecuencia alrededor del momento en que el nuevo valor de RAND se vuelve válido. Al final de la vida útil de un RAND, puede ser necesario radiodifundir tanto el valor de RAND actual como el valor del próximo RAND. Los valores de RAND no deberían ser predecibles, y el CS debería comenzar a enviar RAND solo un corto tiempo antes de que el RAND se haga válido.

**[0105]** Como se analiza anteriormente en el presente documento, de acuerdo con el tercer modo de realización ejemplar, la SK se deriva de BAK, la hora del sistema y un valor aleatorio de radiodifusión denominado SK_RAND. La FIG. 7C ilustra un procedimiento de actualización de claves para el cifrado de seguridad en un sistema de comunicación inalámbrica que admite el servicio de radiodifusión. El procedimiento 440 implementa períodos de tiempo como se indica en la FIG. 7E. La BAK se actualiza periódicamente con un período de tiempo T1. Se inicia un temporizador t1 cuando se calcula la BAK y se agota el tiempo de espera en T1. Se usa una variable para calcular la SK denominada SK_RAND, que se actualiza periódicamente con un período de tiempo T2. Se inicia un temporizador t2 cuando se genera el SK_RAND y se agota el tiempo de espera en T2. En un modo de realización, la SK se actualiza además periódicamente con un período de T3. Se inicia un temporizador t3 cuando se genera cada SK y se agota el tiempo de espera en el tiempo T3. El SK_RAND se genera en el CS y se proporciona periódicamente a la MS. La MS y el CS usan el SK_RAND para generar la SK, como se detalla a continuación en el presente documento.

**[0106]** Un primer temporizador t1 se restablece cuando se actualiza el valor aplicable de BAK. El intervalo entre dos actualizaciones de BAK es el período de actualización de BAK. En el modo de realización ejemplar, el período de actualización de BAK es de un mes, sin embargo, los modos de realización alternativos pueden implementar cualquier período de tiempo deseado para el funcionamiento óptimo del sistema o para satisfacer una variedad de criterios del sistema.

**[0107]** Continuando con la FIG. 7C, el procedimiento 440 inicializa el temporizador t2 en la etapa 442 para iniciar el período de tiempo de SK_REG T2. El CS genera el SK_RAND y proporciona el valor para transmitir los circuitos para la transmisión a través del sistema en la etapa 444. El temporizador t3 se inicializa en la etapa 446 para iniciar el período de tiempo de SK T3 el CS genera la SK a partir de SK-RAND, BAK y TIME en la etapa 448. A continuación, el CS cifra el BC usando la SK actual en la etapa 450. El producto cifrado es el EBC, en el que el CS proporciona el EBC para transmitir circuitos para su transmisión en el sistema. Si el temporizador t2 ha caducado en el rombo de decisión 452, el procesamiento regresa a la etapa 442. Mientras que t2 es menor que T2, si el temporizador t3 ha caducado en el rombo de decisión 452, el procesamiento regresa a la etapa 446, de lo contrario el procesamiento regresa a 450.

**[0108]** La FIG. 7D ilustra el funcionamiento de la MS que accede a un servicio de radiodifusión. El procedimiento 460 sincroniza primero los temporizadores t2 y t3 con los valores en el CS en la etapa 462. El UIM de la MS recibe el SK_RAND generado por el CS en la etapa 464. En la etapa 466, el UIM genera la SK usando el SK_RAND, BAK y una medición de tiempo. El UIM transfiere la SK al ME de la MS. A continuación, el UIM descifra el EBC recibido usando la SK para extraer el BC original en la etapa 468. Cuando el temporizador t2 caduca en la etapa 470, el procesamiento regresa a la etapa 462. Mientras que el temporizador t2 sea menor que T2, si el temporizador t3 caduca en la etapa 472, el temporizador t3 se inicializa en la etapa 474 y regresa a 466.

**[0109]** La FIG. 7E es un diagrama de temporización de los períodos de actualización de clave de una opción de seguridad en un sistema de comunicación inalámbrica que admite transmisiones de radiodifusión.

**[0110]** La gestión de claves y las actualizaciones se ilustran en la FIG. 8C, en las que el CS aplica una función 508 para generar un valor de SK_RAND, que es un valor intermedio usado por el CS y la MS para calcular la SK. Específicamente, la función 508 aplica el valor de BAK, el SK_RAND y un factor de tiempo. Mientras que el modo de realización ilustrado en la FIG. 8C aplica un temporizador para determinar cuándo actualizar la SK, los modos de realización alternativos pueden usar medidas alternativas para proporcionar actualizaciones periódicas, por ejemplo, la ocurrencia de un error u otro acontecimiento. El CS proporciona el valor de SK_RAND a cada uno de los abonados, en el que una función 518 o 538 residente en cada UIM aplica la misma función que en la función 508 del CS. La función 518 funciona en el SK_RAND, la BAK y un valor de temporizador para generar una SK que está almacenada en una localización de memoria en el ME, tal como $MEM_1$ 542 de $ME_1$ 540 y $MEM_N$ 552 de $ME_N$ 550.

**[0111]** Como se analiza anteriormente en el presente documento, de acuerdo con el cuarto modo de realización ejemplar, la SK se cifra usando la BAK para formar la SKI, y la SKI se envía a la MS. En un modo de realización ejemplar, la SK se envía en un paquete de IPSec cifrado usando la BAK. El CS también puede radiodifundir un SPI

correspondiente que se puede usar para identificar datos que se cifran usando la SK. Este modo de realización no necesita ser analizado con más detalle.

**[0112]** En los modos de realización ejemplares proporcionados anteriormente en el presente documento, el CS puede elegir actualizar la SK como lo desee el CS. Cuanto más a menudo cambia la SK, más puede el CS disuadir a los atacantes de distribuir los valores de SK. Habrá momentos en los que un atacante considera que el beneficio de distribuir los valores de SK es mejor que en otros momentos. Esto se debe principalmente a la naturaleza del contenido que se radiodifunde. Por ejemplo, al ocurrir un acontecimiento importante, los usuarios no abonados estarán más interesados en recibir noticias sobre el HSBS y, por lo tanto, estarán dispuestos a pagar más por el acceso ilegítimo que en otros momentos. En estos momentos, el CS puede aumentar el coste y las molestias para el atacante y los usuarios no abonados al cambiar la SK con más frecuencia de lo normal. Sin embargo, el CS debe tener en cuenta los límites de la potencia de procesamiento del UIM. Si el CS cambia la SK con demasiada frecuencia, entonces el UIM no podrá calcular los valores de SK en tiempo real, por lo que los usuarios no podrán descifrar el contenido en tiempo real.

**[0113]** Los expertos en la técnica entenderán que la información y las señales se pueden representar usando cualquiera de una variedad de tecnologías y técnicas diferentes. Por ejemplo, los datos, instrucciones, comandos, información, señales, bits, símbolos y segmentos que se pueden haber referenciado a lo largo de la descripción anterior se pueden representar mediante tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos o cualquier combinación de los mismos.

**[0114]** Los expertos en la técnica apreciarían además que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos divulgados en relación con los modos de realización divulgados en el presente documento se pueden implementar como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y etapas ilustrativas, en general, en lo que respecta a su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de las restricciones particulares de aplicación y de diseño impuestas al sistema global. Los expertos en la técnica pueden implementar la funcionalidad descrita de formas distintas para cada solicitud particular, pero no debería interpretarse que dichas decisiones de implementación suponen apartarse del alcance de la presente invención.

**[0115]** Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con los modos de realización divulgados en el presente documento se pueden implementar o realizar con un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro dispositivo de lógica programable, lógica de transistores o de puertas discretas, componentes de hardware discretos o con cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador, pero de forma alternativa el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

**[0116]** Las etapas de un procedimiento o algoritmo descrito en relación con los modos de realización divulgados en el presente documento se pueden llevar a cabo directamente en el hardware, en un módulo de software ejecutado por un procesador o en una combinación de ambos. Un módulo de software puede residir en una memoria RAM, en una memoria flash, en una memoria ROM, en una memoria EPROM, en una memoria EEPROM, en registros, en un disco duro, en un disco extraíble, en un CD-ROM o en cualquier otro medio de almacenamiento conocido en la técnica. Un medio de almacenamiento ejemplar está acoplado al procesador de modo que el procesador puede leer información de, y escribir información en, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

**[0117]** La descripción anterior de los modos de realización divulgados se proporciona para permitir que cualquier experto en la técnica realice o use la presente invención. Diversas modificaciones de estos modos de realización resultarán fácilmente evidentes a los expertos en la técnica, y los principios genéricos definidos en el presente documento pueden aplicarse a otros modos de realización sin apartarse del alcance de la invención como se define en las reivindicaciones adjuntas.

**REIVINDICACIONES**

**1.** Un procedimiento para transmisiones seguras en un canal de radiodifusión, comprendiendo el procedimiento:

obtener (714) una clave a corto plazo (800) para un mensaje para su transmisión, correspondiendo la clave a corto plazo a un identificador de clave a corto plazo;

determinar (702) una clave de acceso de radiodifusión para el mensaje, correspondiendo la clave de acceso de radiodifusión a un identificador de clave de acceso (804);

cifrar (716) el mensaje con la clave a corto plazo;

formar (718) una cabecera de protocolo de Internet que comprenda el identificador de clave a corto plazo; y

transmitir (718) el mensaje cifrado en el canal de radiodifusión con la cabecera de protocolo de Internet, en el que la clave a corto plazo (714) se calcula en función del identificador de clave a corto plazo y de la clave de acceso de radiodifusión.

**2.** El procedimiento de la reivindicación 1, en el que el identificador de clave a corto plazo comprende el identificador de clave de acceso (804).

**3.** El procedimiento de la reivindicación 2, en el que el identificador de clave a corto plazo comprende además un valor de índice de parámetros de seguridad.

**4.** El procedimiento de la reivindicación 3, en el que el valor de índice de parámetros de seguridad es un número aleatorio (806).

**5.** El procedimiento de la reivindicación 1, en el que el identificador de clave a corto plazo se calcula (714) cifrando el identificador de clave a corto plazo con la clave de acceso de radiodifusión.

**6.** El procedimiento de la reivindicación 1, en el que la cabecera de protocolo de Internet es parte de una cabecera ESP.

**7.** El procedimiento de la reivindicación 6, en el que la cabecera de protocolo de Internet comprende además un segundo número aleatorio, teniendo el segundo número aleatorio un identificador de número aleatorio.

**8.** El procedimiento de la reivindicación 7, en el que el identificador de clave a corto plazo comprende el identificador de clave de acceso y el identificador de número aleatorio.

**9.** El procedimiento de la reivindicación 8, en el que el identificador de clave a corto plazo comprende además un valor de índice de parámetros de seguridad.

**10.** El procedimiento de la reivindicación 9, en el que el valor de índice de parámetros de seguridad es un número aleatorio.

**11.** El procedimiento de la reivindicación 7, en el que la clave a corto plazo se calcula en función del identificador de clave a corto plazo, del segundo número aleatorio y de la clave de acceso de radiodifusión.

**12.** El procedimiento de la reivindicación 11, en el que el identificador de clave a corto plazo se calcula cifrando el identificador de clave a corto plazo y el segundo número aleatorio con la clave de acceso de radiodifusión.

**13.** Un procedimiento para recepción de una transmisión en un canal de radiodifusión, comprendiendo el procedimiento:

recibir (752) un identificador de clave a corto plazo específico para una transmisión, correspondiendo el identificador de clave a corto plazo a una clave a corto plazo;

determinar (758) una clave de acceso de radiodifusión en base al identificador de clave a corto plazo;

cifrar (764) el identificador de clave a corto plazo con la clave de acceso de radiodifusión para recuperar la clave a corto plazo; y

descifrar (766) la transmisión en el canal de radiodifusión usando la clave a corto plazo.

**14.** El procedimiento de la reivindicación 13, que comprende además:

almacenar el identificador de clave a corto plazo y la clave a corto plazo en una unidad de almacenamiento de memoria (306).

**15.** El procedimiento de la reivindicación 13, en el que el identificador de clave a corto plazo está compuesto de un número aleatorio (806) y de un identificador de clave de acceso asociado con la clave de acceso de radiodifusión.

**16.** El procedimiento de la reivindicación 13, en el que cifrar el identificador de clave a corto plazo comprende además cifrar el identificador de clave a corto plazo y un número aleatorio con la clave de acceso de radiodifusión para recuperar la clave a corto plazo.

**17.** Un elemento de infraestructura para un sistema de comunicación inalámbrica (200) que usa un canal de radiodifusión que comprende:

medios para recibir (304) un identificador de clave a corto plazo específico para una transmisión en el canal de radiodifusión, correspondiendo el identificador de clave a corto plazo a una clave a corto plazo;

medios para determinar una clave de acceso de radiodifusión en base al identificador de clave a corto plazo;

medios para cifrar el identificador de clave a corto plazo con la clave de acceso de radiodifusión para recuperar la clave a corto plazo; y

medios para descifrar la transmisión en el canal de radiodifusión usando la clave a corto plazo.

**18.** Un medio legible por ordenador, que comprende instrucciones que, cuando se ejecutan por un ordenador, causan que el ordenador lleve a cabo los pasos del procedimiento de cualquiera de las reivindicaciones 1 a 16.

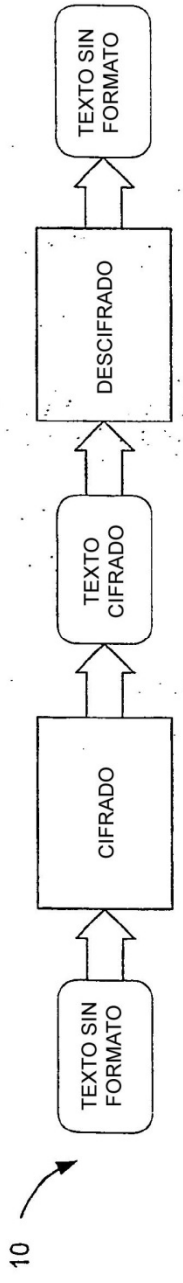


FIG. 1A

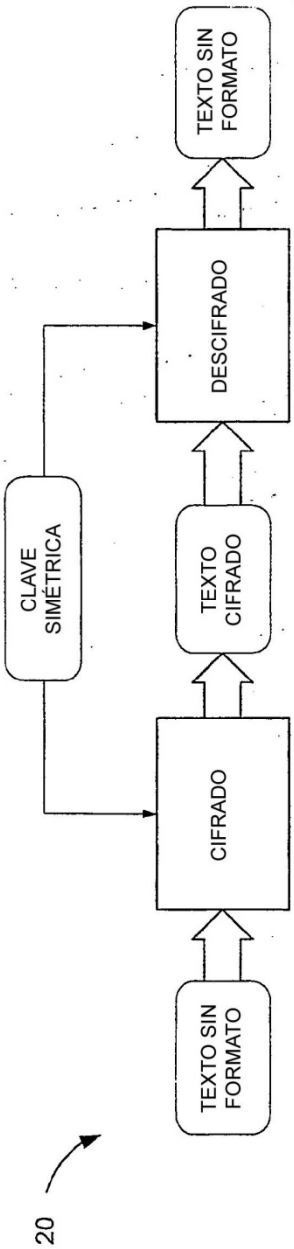


FIG. 1B

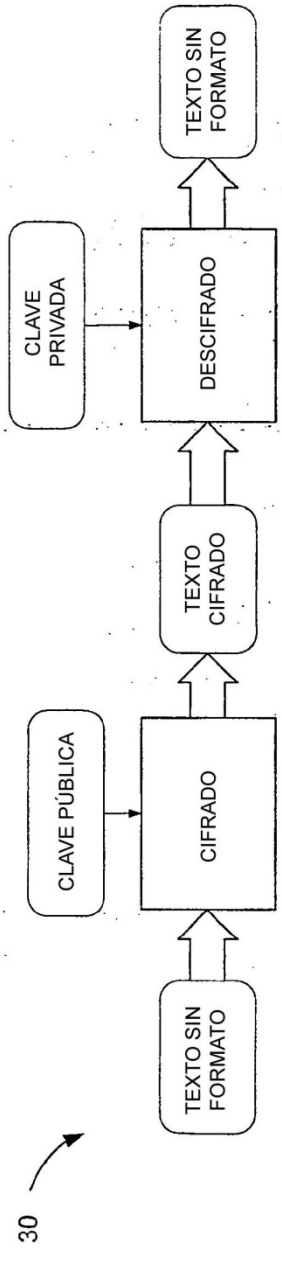


FIG. 1C

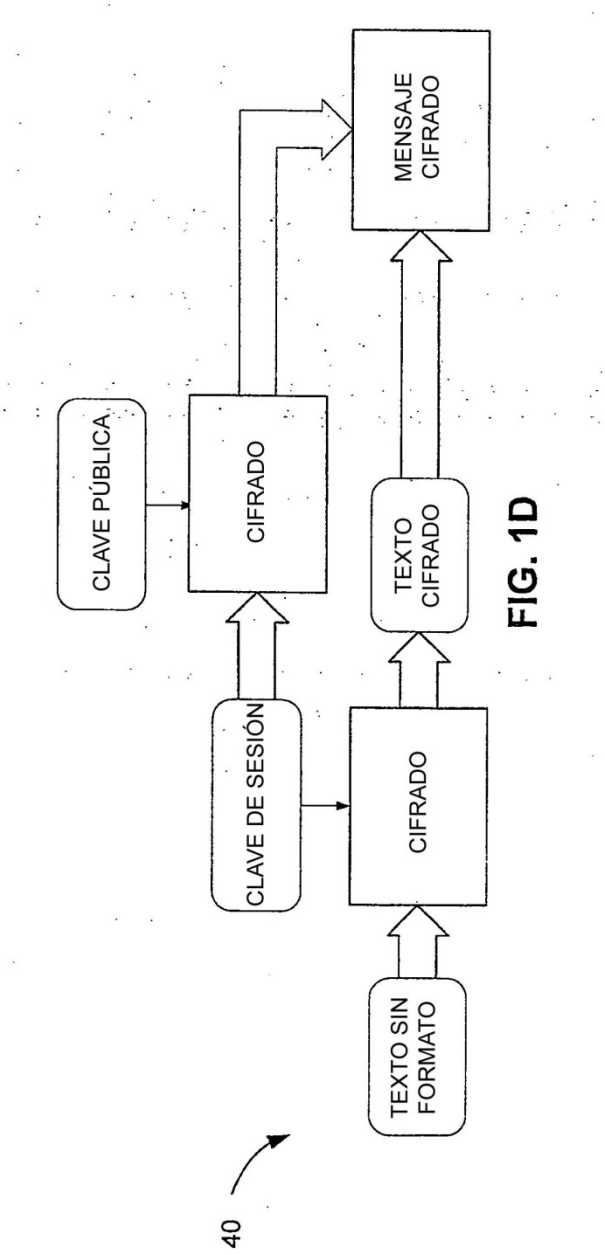
MENSAJE CIFRADO
CLAVE PÚBLICA
CIFRADO
TEXTO CIFRADO
CLAVE DE SESIÓN
CIFRADO
TEXTO SIN FORMATO
40

FIG. 1D

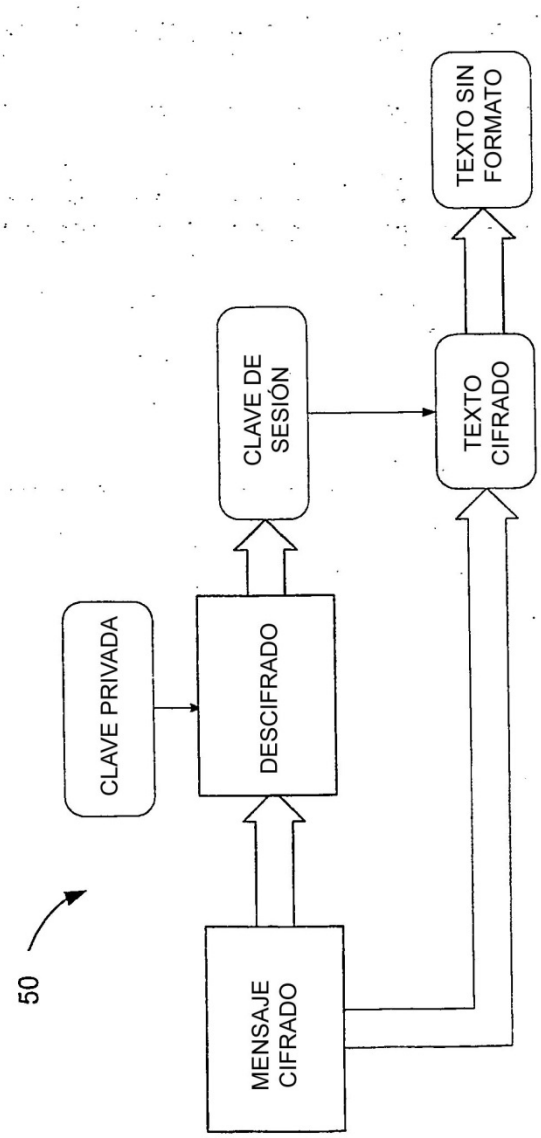
50
MENSAJE CIFRADO
CLAVE PRIVADA
DESCIFRADO
CLAVE DE SESIÓN
TEXTO CIFRADO
TEXTO SIN FORMATO

FIG. 1E

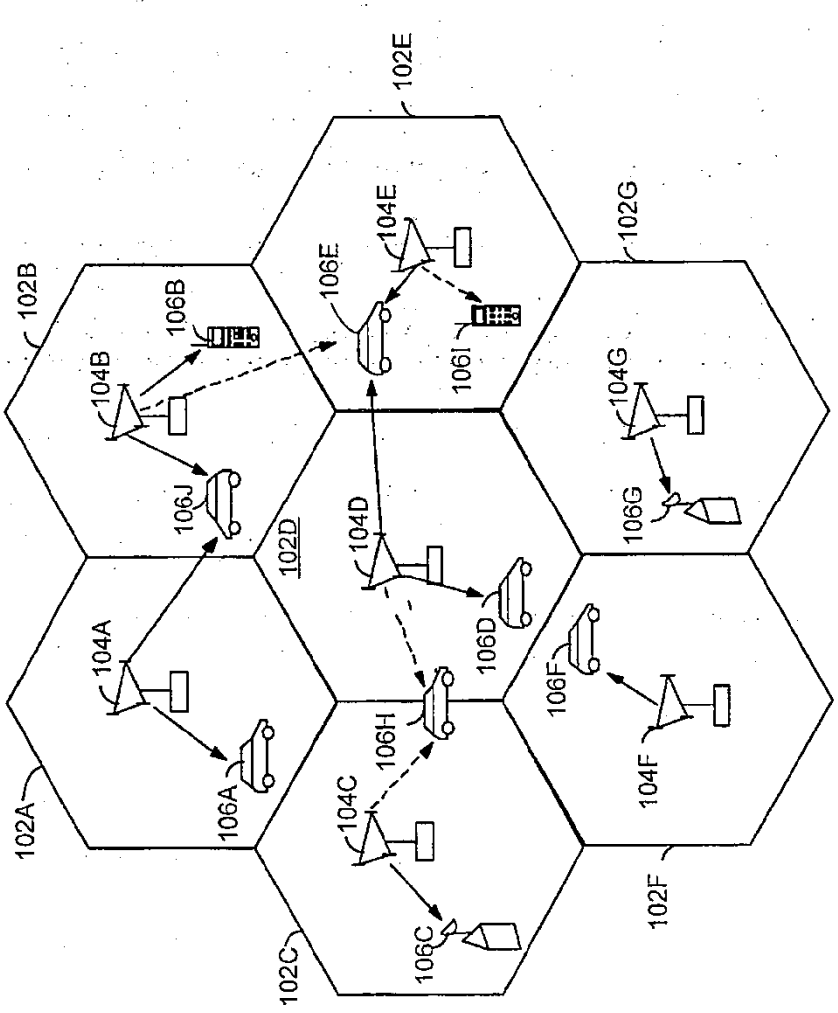
100
102A
102B
102C
102D
102E
102F
102G
104A
104B
104C
104D
104E
104F
104G
106A
106B
106C
106D
106E
106F
106G
106H
106I
106J

FIG. 2

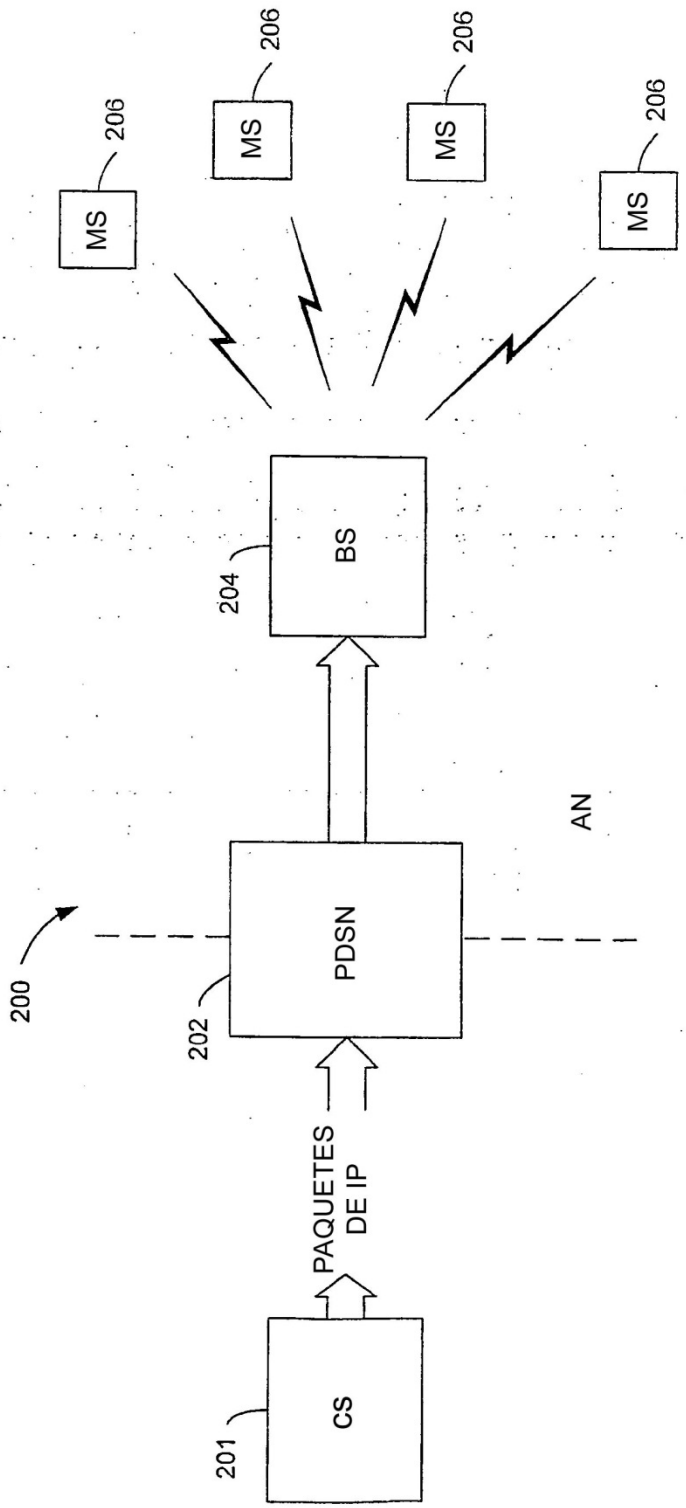
206
206
206
MS
MS
MS
MS
BS
204
AN
PDSN
200
202
PAQUETES DE IP
CS
201

FIG. 3

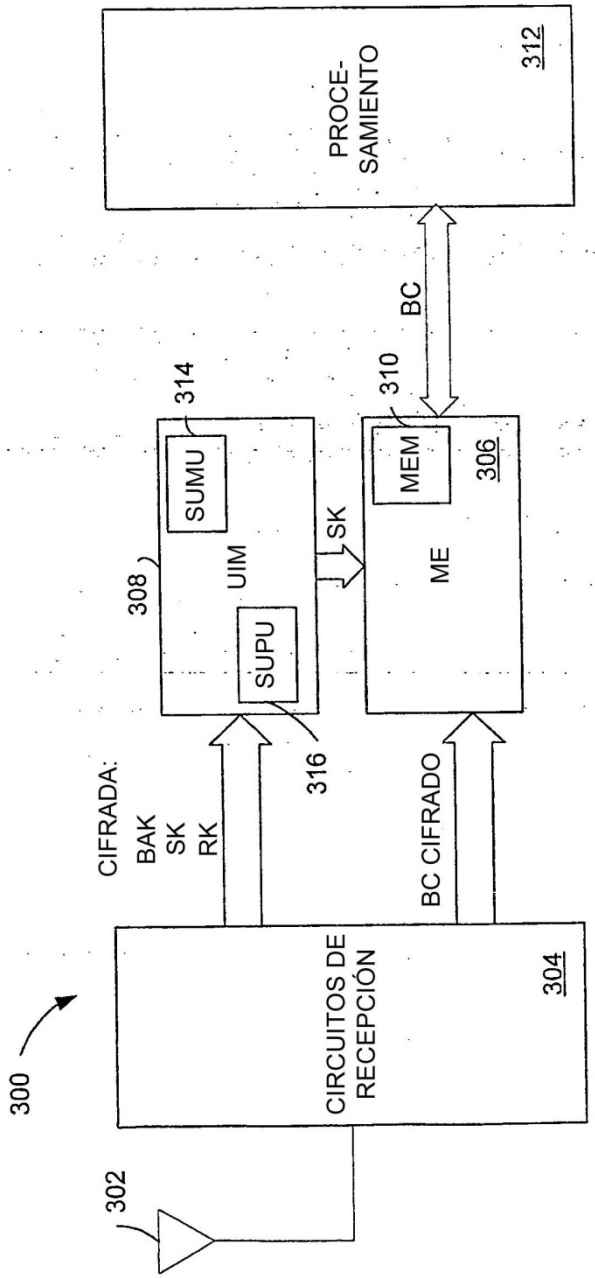
PROCE-
SAMIENTO
312
BC
314
310
SUMU
MEM
306
SK
308
UIM
ME
SUPU
316
CIFRADA:
BAK
SK
RK
BC CIFRADO
CIRCUITOS DE
RECEPCIÓN
304
300
302

FIG. 4

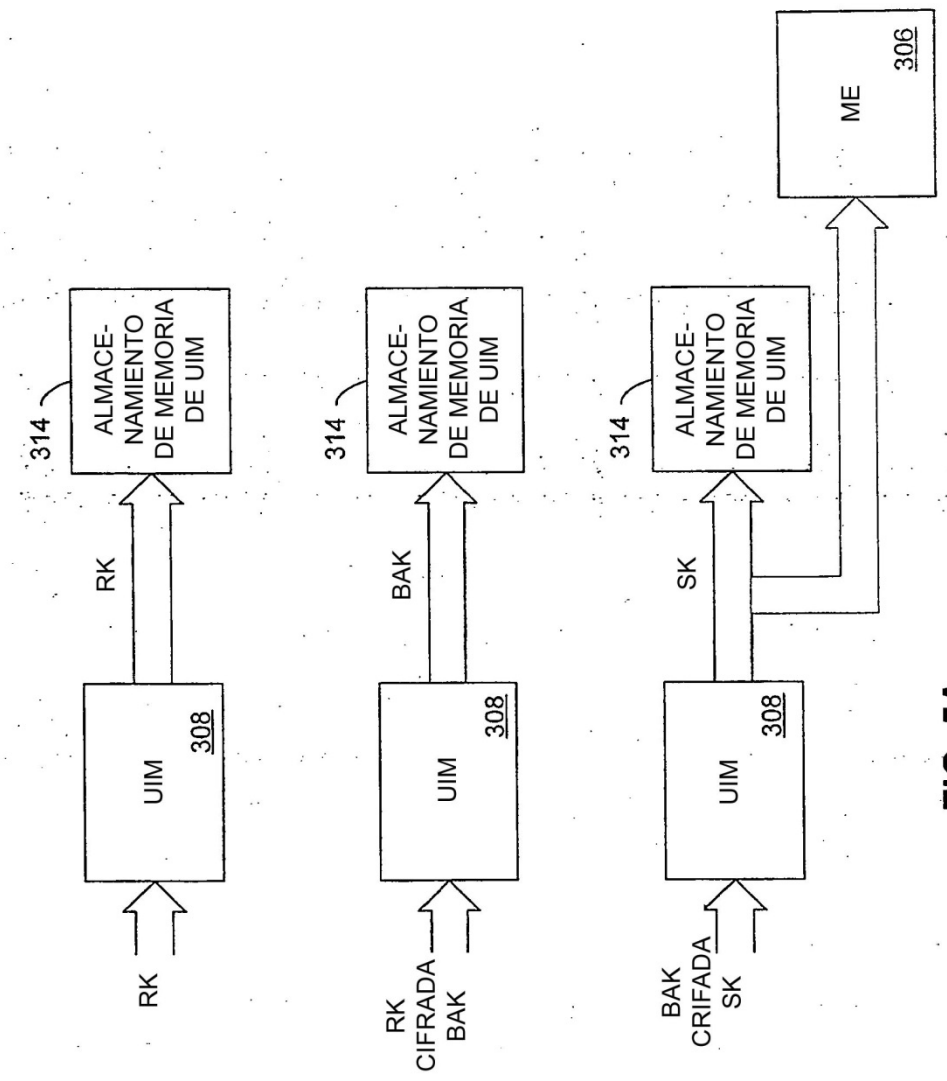
RK
UIM
308
RK
314
ALMACE-
NAMIENTO
DE MEMORIA
DE UIM
RK
CIFRADA
BAK
UIM
308
BAK
314
ALMACE-
NAMIENTO
DE MEMORIA
DE UIM
BAK
CRIFADA
SK
UIM
308
SK
314
ALMACE-
NAMIENTO
DE MEMORIA
DE UIM
ME
306

FIG. 5A

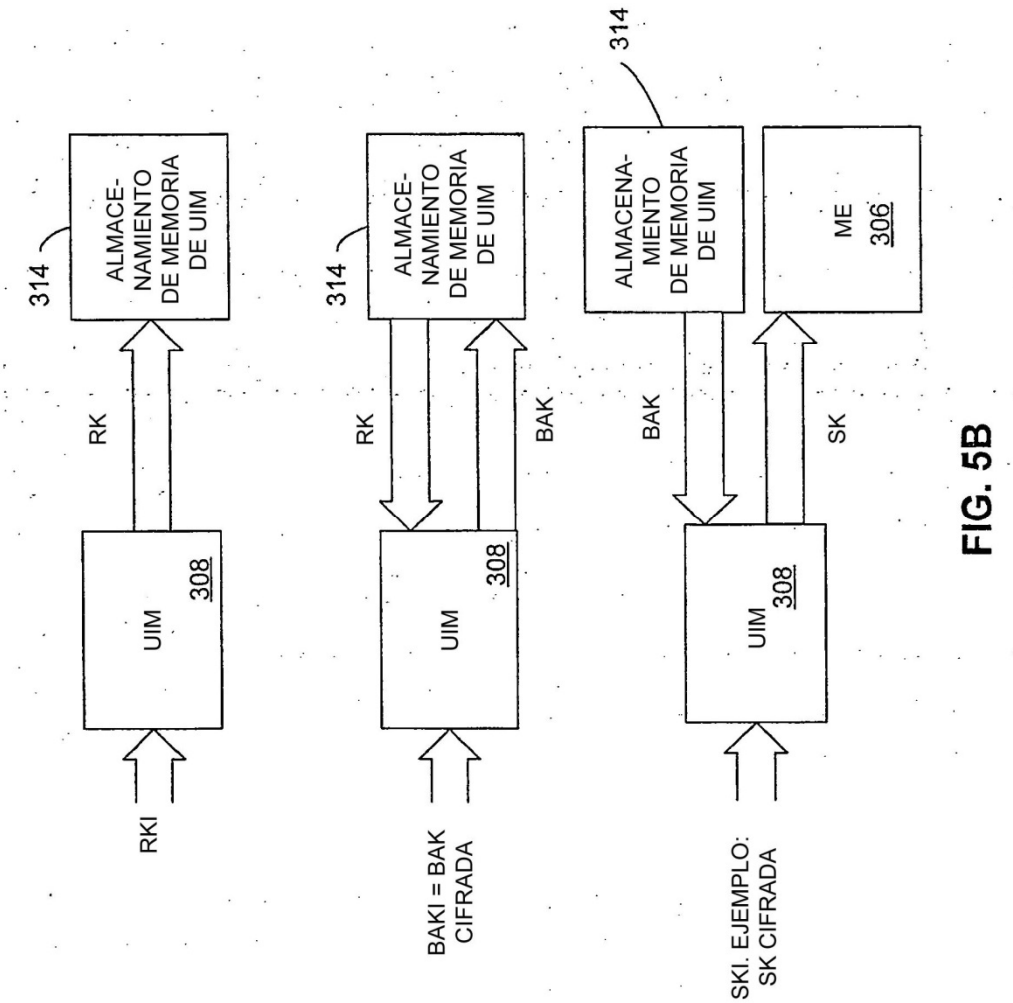
314
ALMACE-NAMIENTO DE MEMORIA DE UIM
RK
UIM
308
RKI
314
ALMACE-NAMIENTO DE MEMORIA DE UIM
RK
BAK
UIM
308
BAKI = BAK CIFRADA
314
ALMACENA-MIENTO DE MEMORIA DE UIM
ME
306
BAK
SK
UIM
308
SKI. EJEMPLO: SK CIFRADA

FIG. 5B

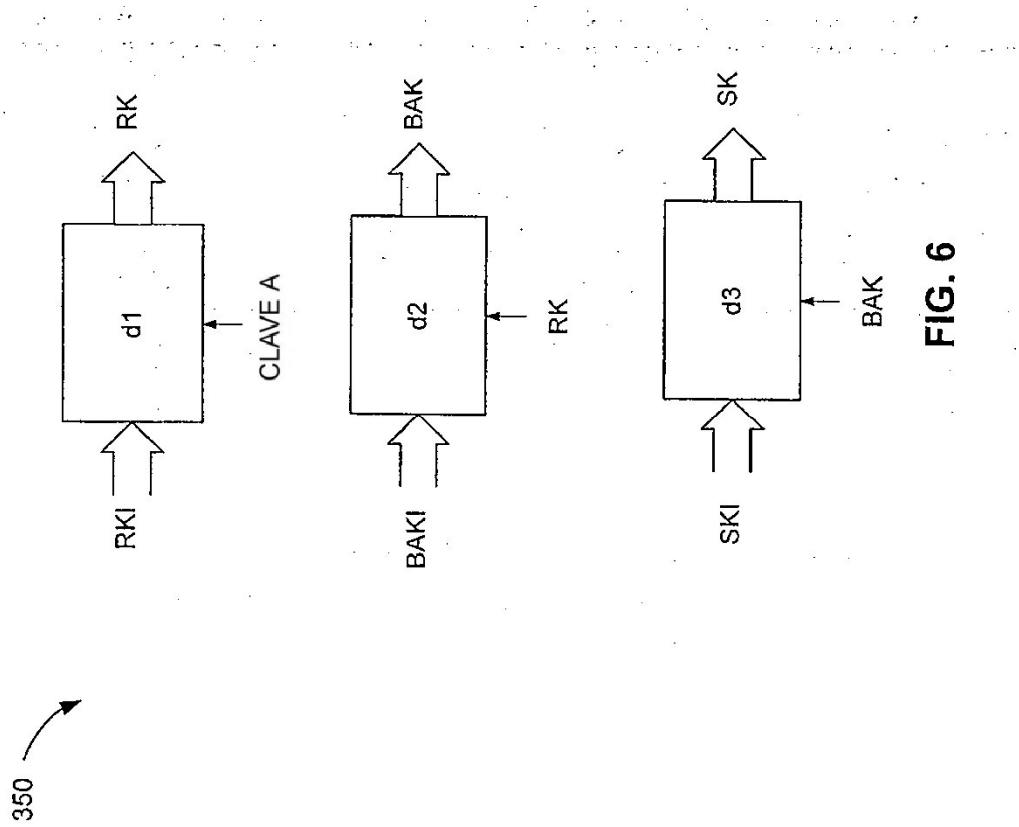


FIG. 6

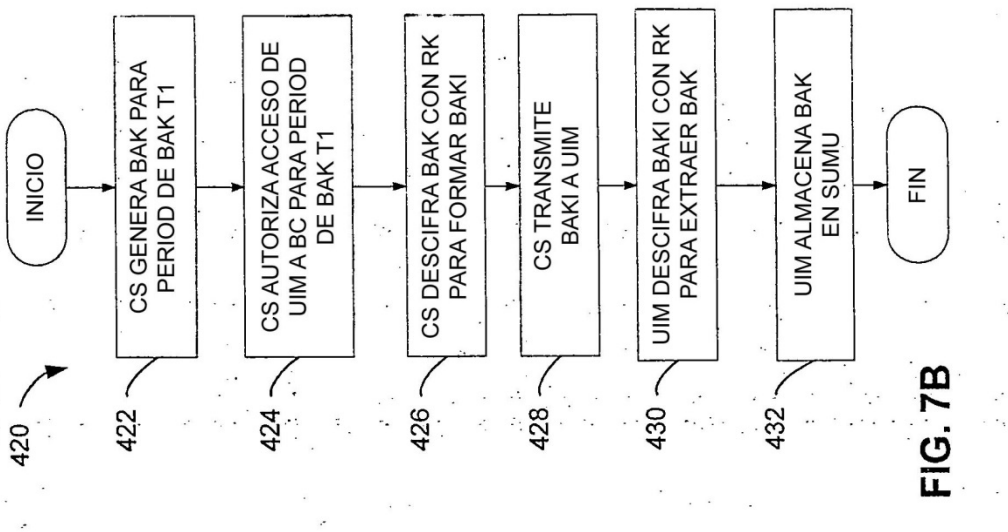
420
INICIO
422
CS GENERA BAK PARA PERIOD DE BAK T1
424
CS AUTORIZA ACCESO DE UIM A BC PARA PERIOD DE BAK T1
426
CS DESCIFRA BAK CON RK PARA FORMAR BAKI
428
CS TRANSMITE BAKI A UIM
430
UIM DESCIFRA BAKI CON RK PARA EXTRAER BAK
432
UIM ALMACENA BAK EN SUMU
FIN

FIG. 7B

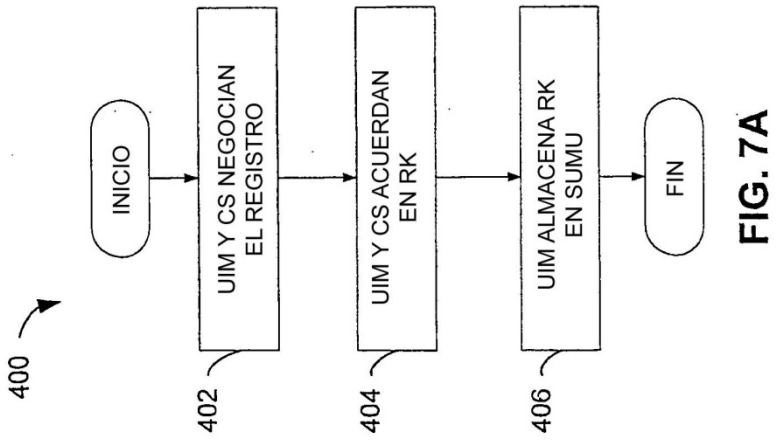
400
INICIO
402
UIM Y CS NEGOCIAN EL REGISTRO
404
UIM Y CS ACUERDAN EN RK
406
UIM ALMACENA RK EN SUMU
FIN

FIG. 7A

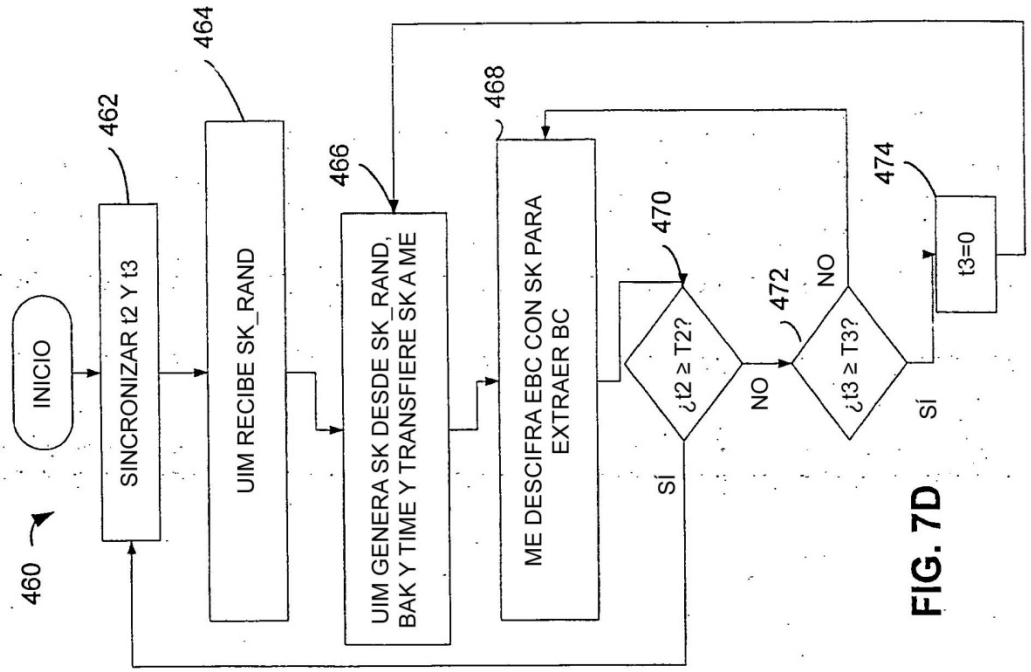
460
INICIO
462
SINCRONIZAR t2 Y t3
464
UIM RECIBE SK_RAND
466
UIM GENERA SK DESDE SK_RAND, BAK Y TIME Y TRANSFIERE SK A ME
468
ME DESCIFRA EBC CON SK PARA EXTRAER BC
470
¿t2 ≥ T2?
SÍ
NO
472
¿t3 ≥ T3?
NO
SÍ
474
t3=0

FIG. 7D

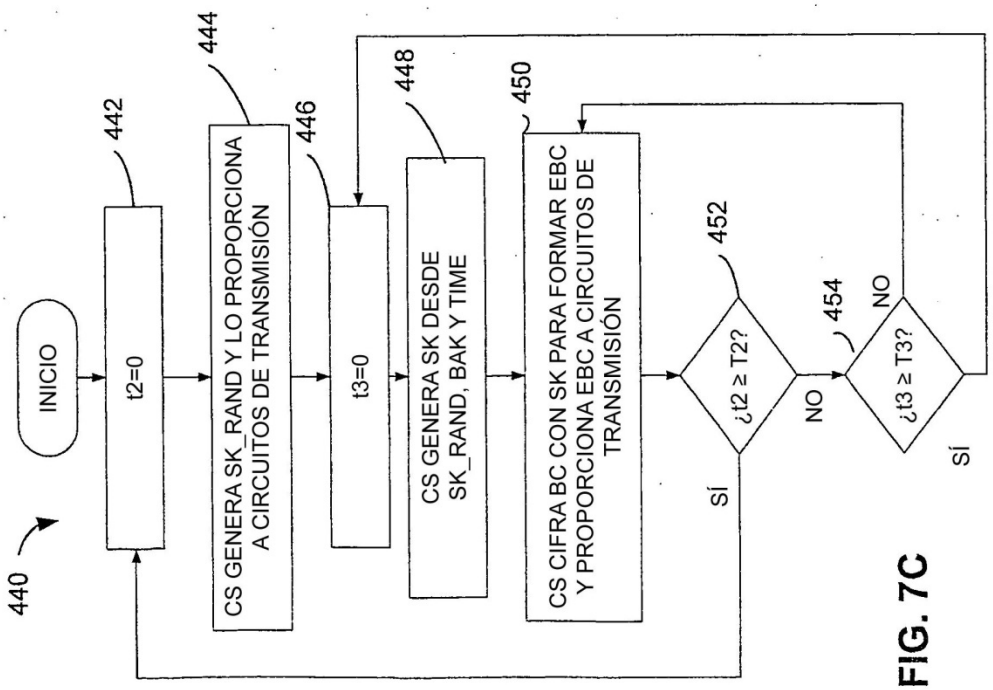
440
INICIO
442
t2=0
444
CS GENERA SK_RAND Y LO PROPORCIONA A CIRCUITOS DE TRANSMISIÓN
446
t3=0
448
CS GENERA SK DESDE SK_RAND, BAK Y TIME
450
CS CIFRA BC CON SK PARA FORMAR EBC Y PROPORCIONA EBC A CIRCUITOS DE TRANSMISIÓN
452
¿t2 ≥ T2?
SÍ
NO
454
¿t3 ≥ T3?
NO
SÍ

FIG. 7C

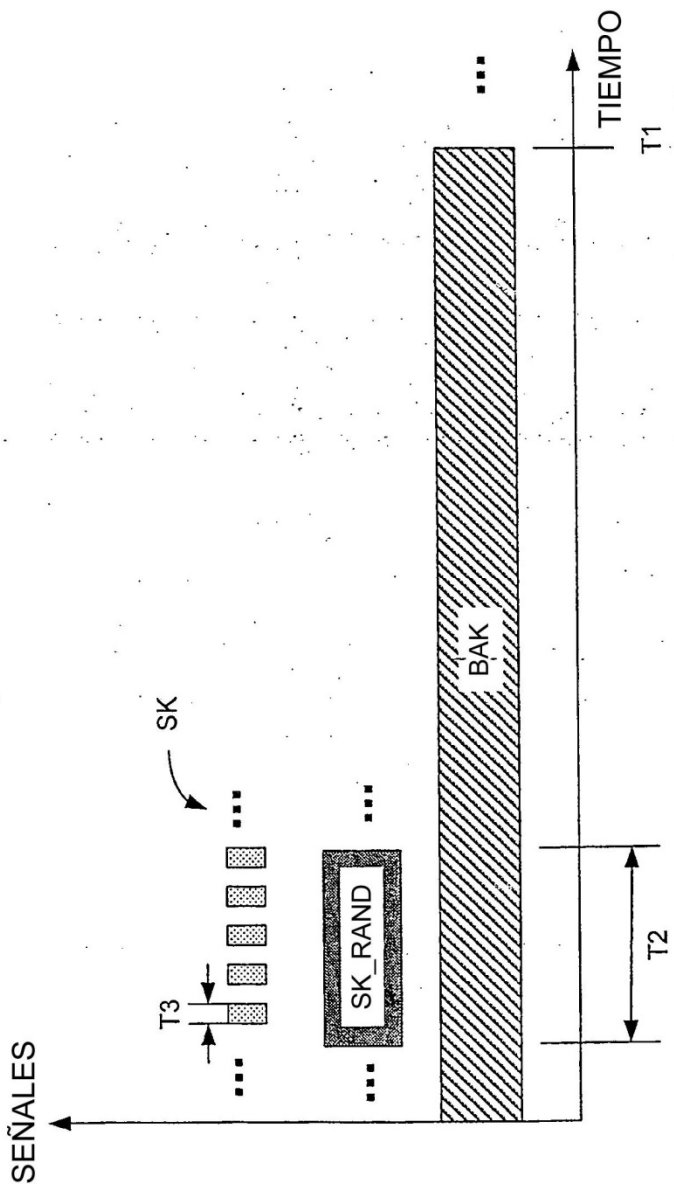


FIG. 7E

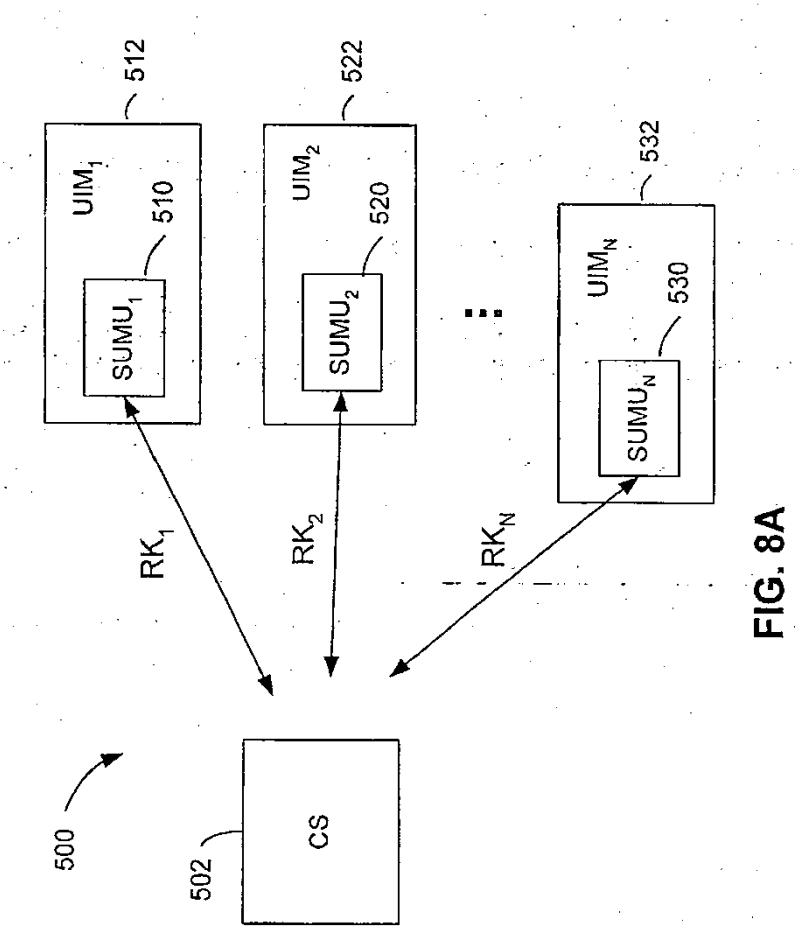
500
CS
502
RK1
RK2
RKN
UIM1
512
SUMU1
510
UIM2
522
SUMU2
520
UIMN
532
SUMUN
530

FIG. 8A

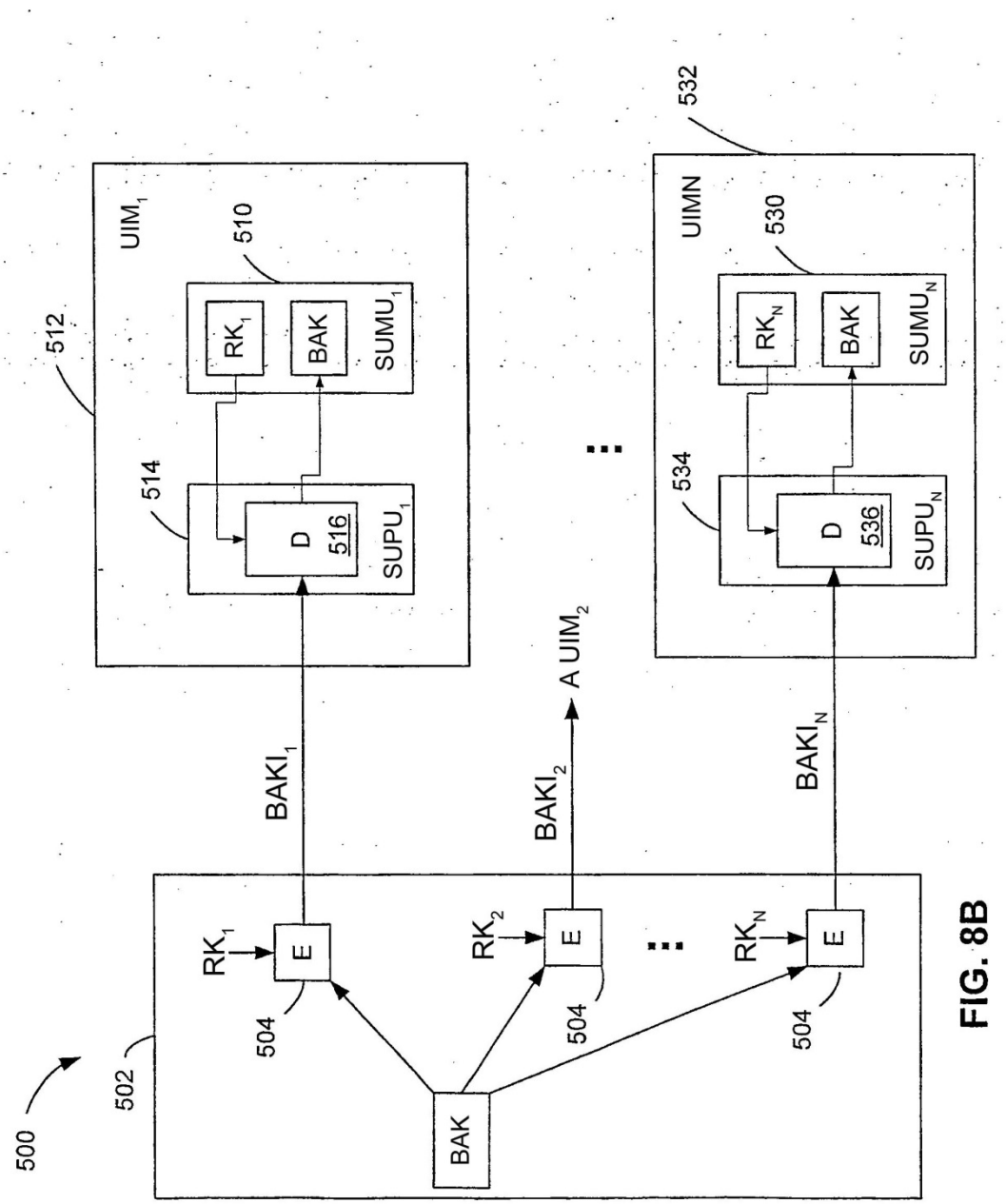
500
502
BAK
RK1
E
504
BAKI1
UIM1
512
514
SUPU1
D
516
RK1
BAK
SUMU1
510
RK2
E
504
BAKI2
A UIM2
RKN
E
504
BAKIN
UIMN
532
534
SUPUN
D
536
RKN
BAK
SUMUN
530

FIG. 8B

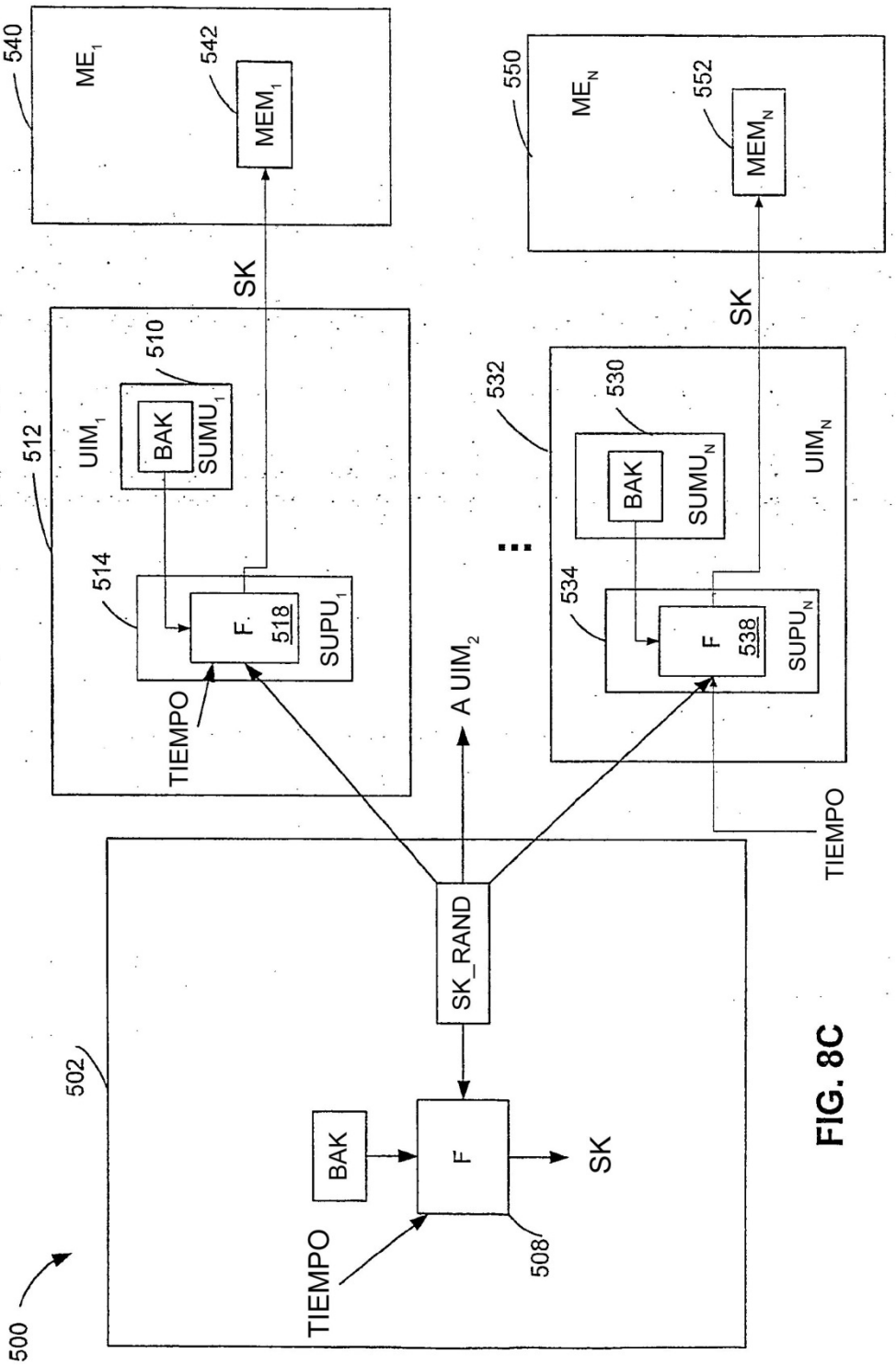
500
502
BAK
F
SK
TIEMPO
508
SK_RAND
A UIM2
TIEMPO
ME1
540
MEM1
542
SK
UIM1
512
BAK
SUMU1
510
514
F
518
SUPU1
TIEMPO
MEN
550
MEMN
552
SK
UIMN
532
BAK
SUMUN
530
534
F
538
SUPUN
TIEMPO

FIG. 8C

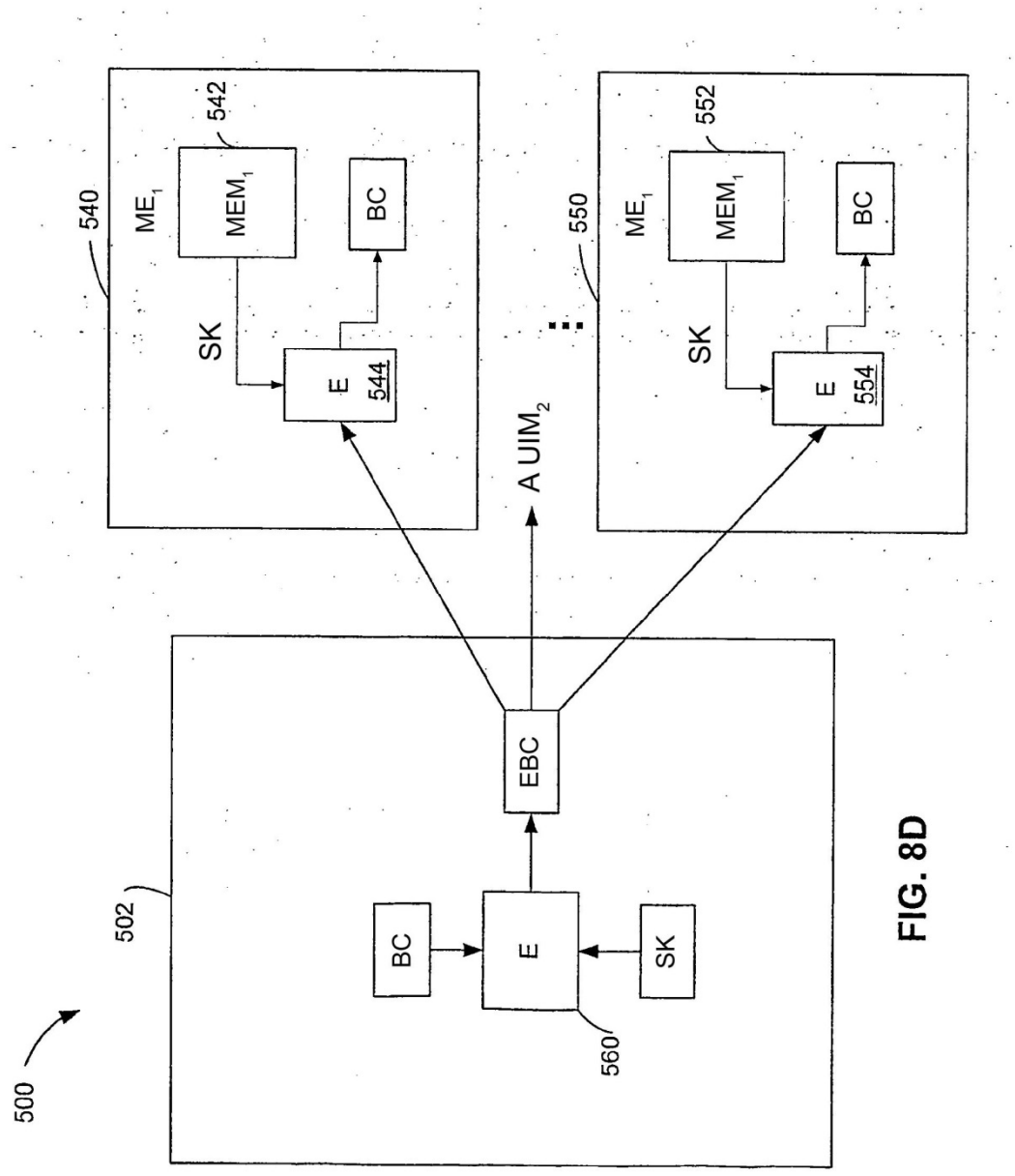
500
502
BC
E
SK
560
EBC
A UIM2
540
ME1
MEM1
542
BC
SK
E
544
550
ME1
MEM1
552
BC
SK
E
554

FIG. 8D

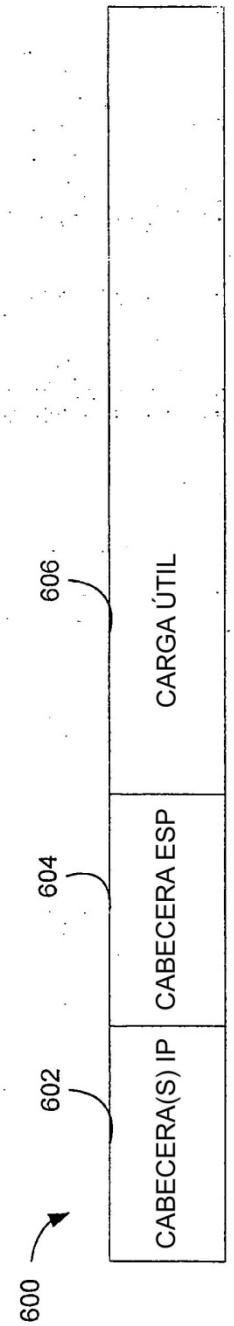
600
602
CABECERA(S) IP
604
CABECERA ESP
606
CARGA ÚTIL

FIG. 9A

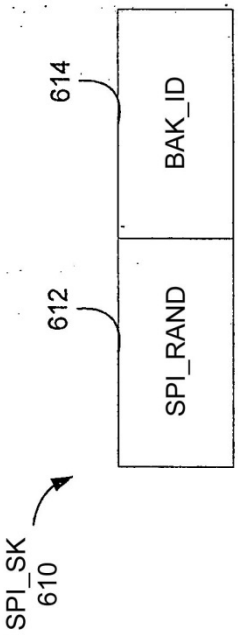
SPI_SK
610
612
SPI_RAND
614
BAK_ID

FIG. 9B

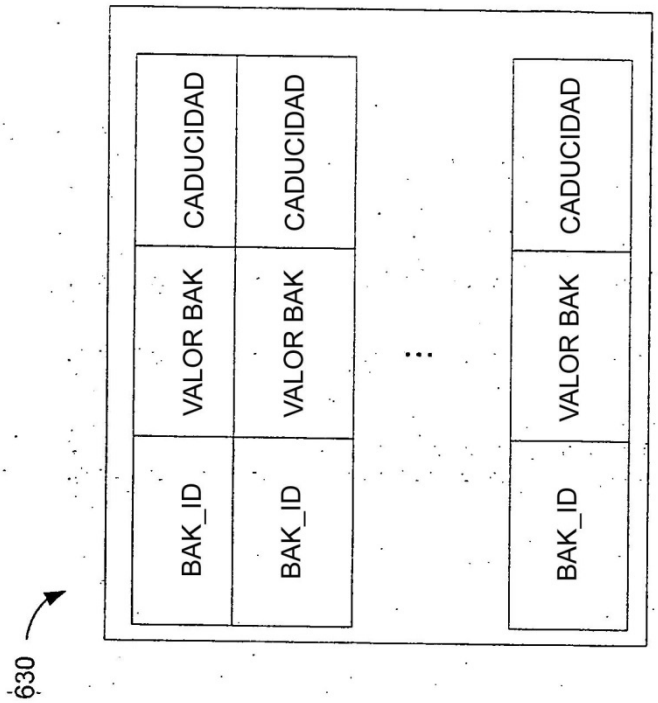
630
BAK_ID
VALOR BAK
CADUCIDAD
BAK_ID
VALOR BAK
CADUCIDAD
BAK_ID
VALOR BAK
CADUCIDAD

FIG. 9D

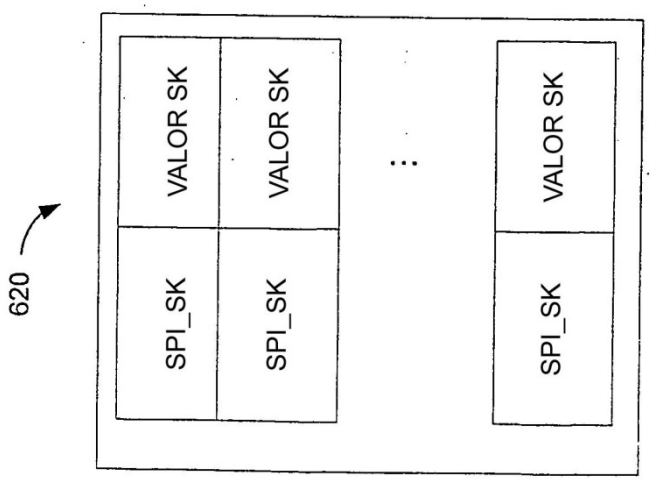
620
SPI_SK
VALOR SK
SPI_SK
VALOR SK
SPI_SK
VALOR SK

FIG. 9C

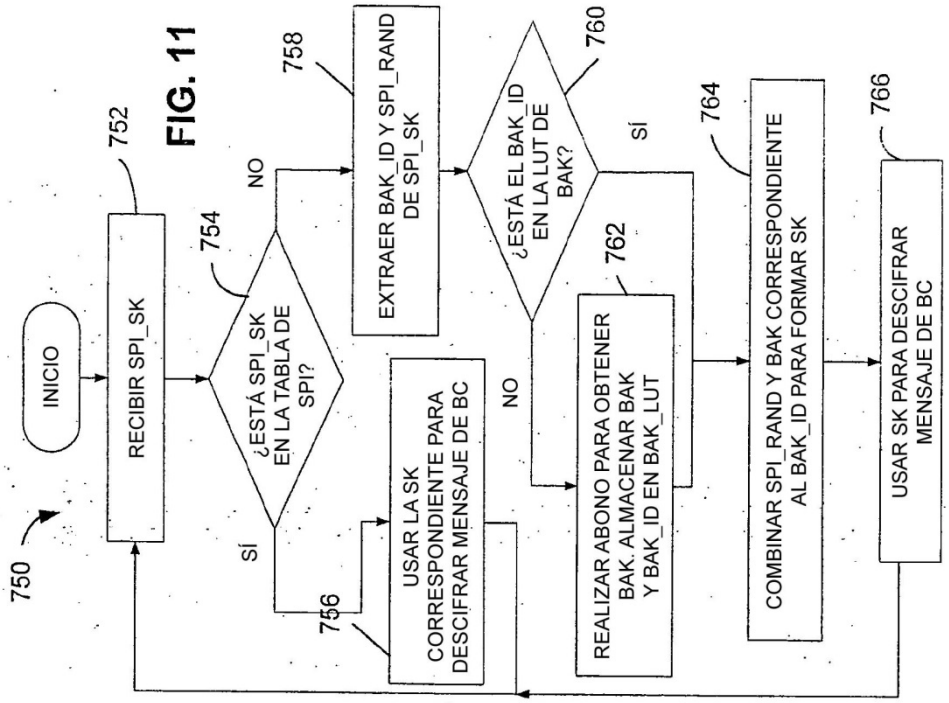
750
INICIO
752
RECIBIR SPI_SK
754
¿ESTÁ SPI_SK EN LA TABLA DE SPI?
SÍ
NO
756
USAR LA SK CORRESPONDIENTE PARA DESCIFRAR MENSAJE DE BC
758
EXTRAER BAK_ID Y SPI_RAND DE SPI_SK
760
¿ESTÁ EL BAK_ID EN LA LUT DE BAK?
SÍ
NO
762
REALIZAR ABONO PARA OBTENER BAK. ALMACENAR BAK Y BAK_ID EN BAK_LUT
764
COMBINAR SPI_RAND Y BAK CORRESPONDIENTE AL BAK_ID PARA FORMAR SK
766
USAR SK PARA DESCIFRAR MENSAJE DE BC

FIG. 11

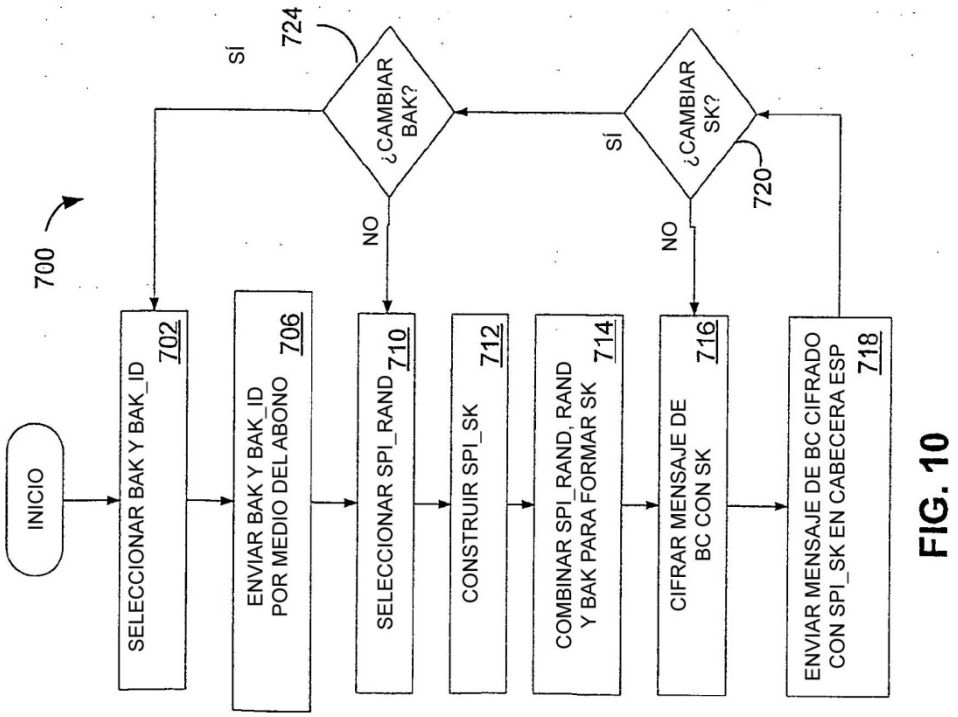
700
INICIO
SELECCIONAR BAK Y BAK_ID
702
ENVIAR BAK Y BAK_ID POR MEDIO DEL ABONO
706
SELECCIONAR SPI_RAND
710
CONSTRUIR SPI_SK
712
COMBINAR SPI_RAND, RAND Y BAK PARA FORMAR SK
714
CIFRAR MENSAJE DE BC CON SK
716
ENVIAR MENSAJE DE BC CIFRADO CON SPI_SK EN CABECERA ESP
718
¿CAMBIAR SK?
720
SÍ
NO
¿CAMBIAR BAK?
724
SÍ
NO

FIG. 10

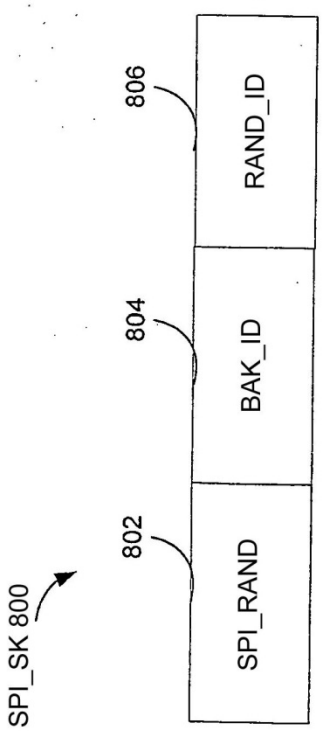


FIG. 12A

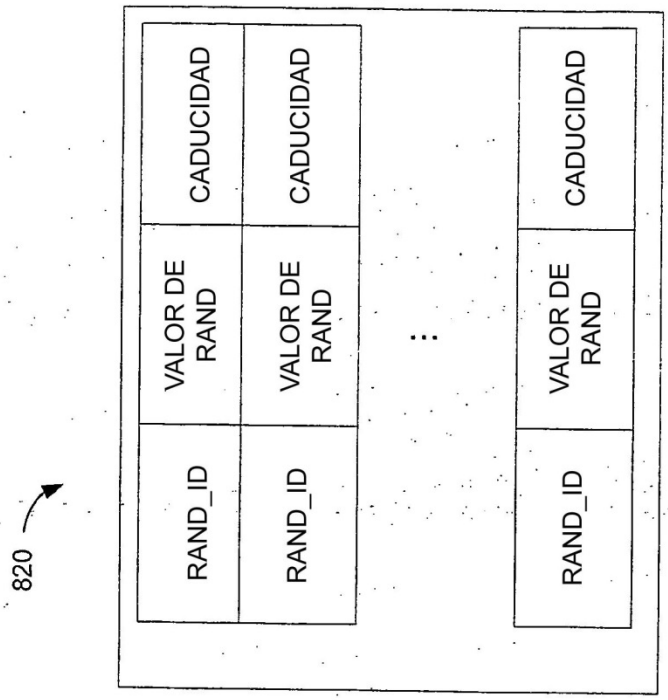


FIG. 12B

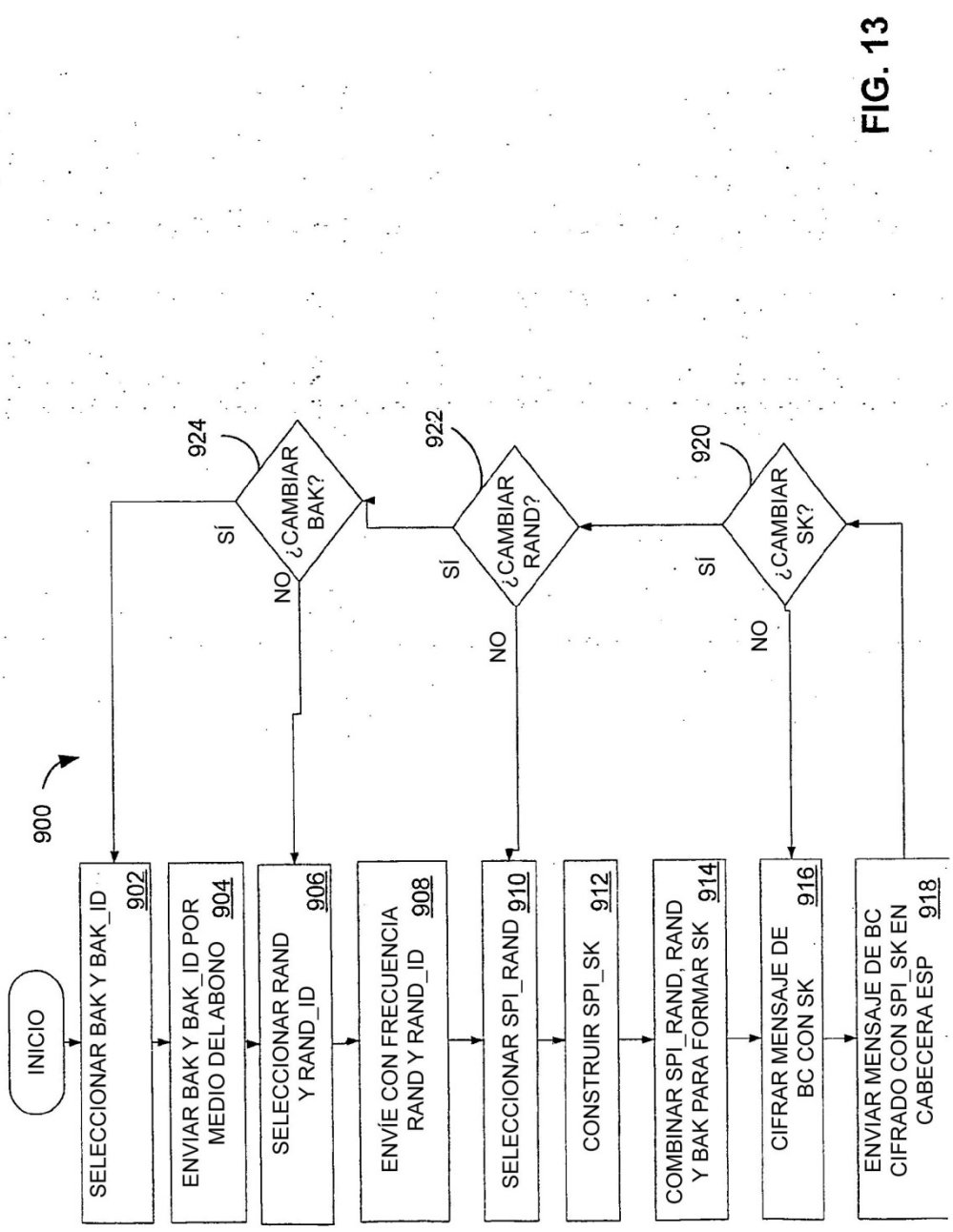
900
INICIO
SELECCIONAR BAK Y BAK_ID 902
ENVIAR BAK Y BAK_ID POR MEDIO DEL ABONO 904
SELECCIONAR RAND Y RAND_ID 906
ENVÍE CON FRECUENCIA RAND Y RAND_ID 908
SELECCIONAR SPI_RAND 910
CONSTRUIR SPI_SK 912
COMBINAR SPI_RAND, RAND Y BAK PARA FORMAR SK 914
CIFRAR MENSAJE DE BC CON SK 916
ENVIAR MENSAJE DE BC CIFRADO CON SPI_SK EN CABECERA ESP 918
920
¿CAMBIAR SK?
SÍ
NO
922
¿CAMBIAR RAND?
SÍ
NO
924
¿CAMBIAR BAK?
SÍ
NO

FIG. 13

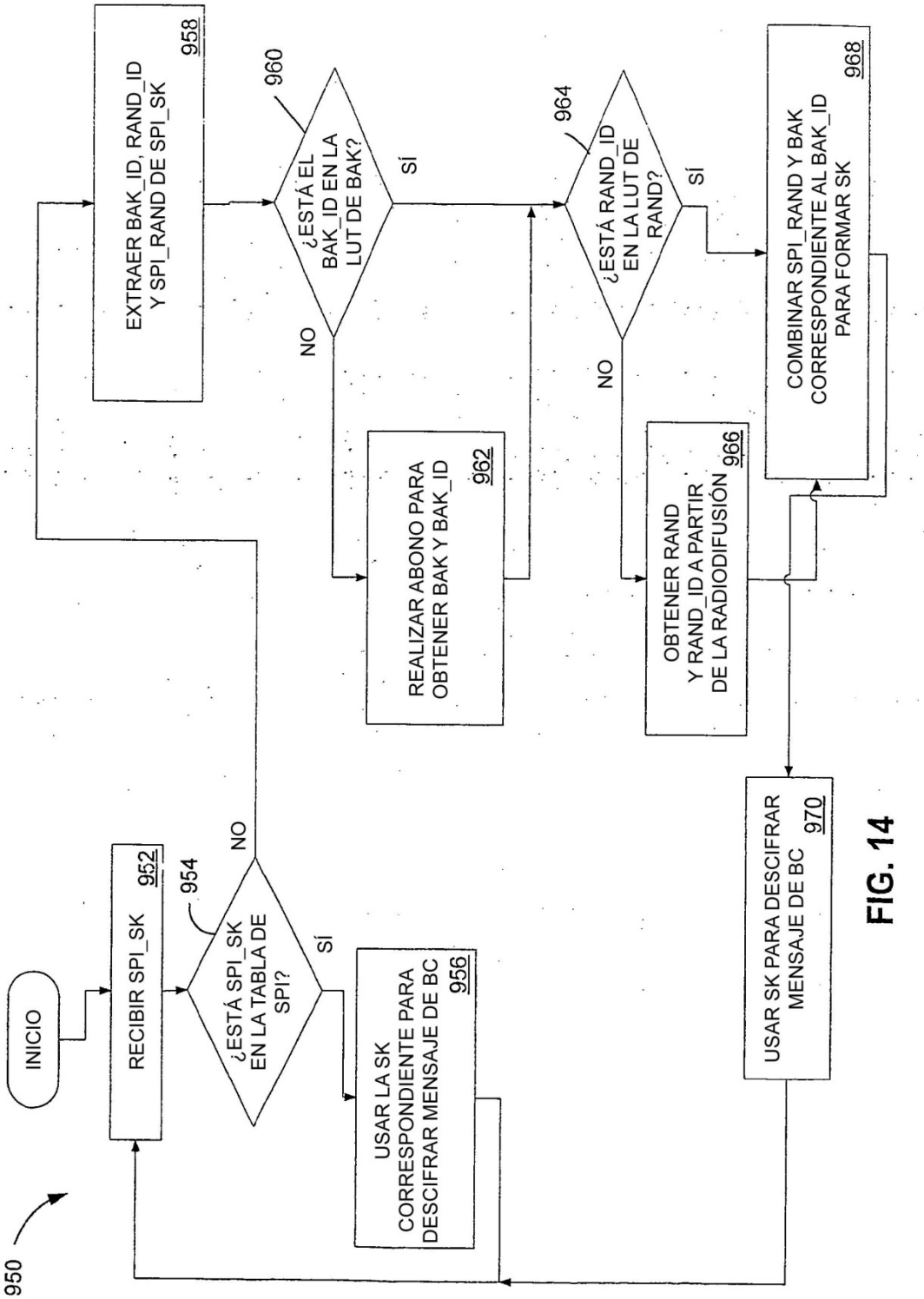
950
INICIO
RECIBIR SPI_SK
952
954
¿ESTÁ SPI_SK EN LA TABLA DE SPI?
NO
SÍ
USAR LA SK CORRESPONDIENTE PARA DESCIFRAR MENSAJE DE BC
956
EXTRAER BAK_ID, RAND_ID Y SPI_RAND DE SPI_SK
958
960
¿ESTÁ EL BAK_ID EN LA LUT DE BAK?
NO
SÍ
REALIZAR ABONO PARA OBTENER BAK Y BAK_ID
962
964
¿ESTÁ RAND_ID EN LA LUT DE RAND?
NO
SÍ
OBTENER RAND Y RAND_ID A PARTIR DE LA RADIODIFUSIÓN
966
COMBINAR SPI_RAND Y BAK CORRESPONDIENTE AL BAK_ID PARA FORMAR SK
968
USAR SK PARA DESCIFRAR MENSAJE DE BC
970

FIG. 14